APPROVAL FORM

The undersigned certify that they have read and recommended to the Midlands State University for acceptance the student MACHAYA VURAMAYI (R11289N)'s dissertation entitled ***"An investigation of the challenges of implementing the Risk Based Internal Auditing (RBIA) in the ZNA"*** which is submitted in partial fulfilment of the requirements of the Bachelor of Commerce Accounting Honours Degree.

Sign……..................................../Date……………………………………………

SUPERVISOR

Sign…………………………………../Date…………………………………………

CHAIRMAN

Sign…………………………………../Date…………………………………………….

EXTERNAL EXAMINER

Sign…………………………………../Date…………………………………………….

LIBRARIAN

RELEASE FORM

NAME OF STUDENT MACHAYA VURAMAYI

TITLE OF DISSERTATION AN INVESTIGATION OF THE CHALLENGES OF IMPLEMENTING THE RISK BASED INTERNAL AUDITING (RBIA) IN THE ZNA.

DEGREE PROGRAMME BACHELOR OF COMMERCE ACCOUNTING HONOURS DEGREE.

YEAR GRANTED SEPTEMBER 2014

Permission is hereby granted to the Midlands State University Library to produce single copies of this Project and to lend such copies for private, scholarly or scientific research purposes only.

The author reserves other publication rights and neither the dissertation extract or any part thereof may be printed or otherwise reproduced without the author`s written permission.

SIGNED ……………………………………………………………………………….

PERMANENT ADDRESS: Stand Number 3535
Maridale, NORTON

DATE SEPTEMBER 2014

DEDICATIONS

My special dedication goes to my lovely wife Memory, son Russell and daughters Tinotenda, Michelle and Rachael. You guys were such an inspiration to me. Without your invaluable support, l could not have managed to reach this milestone. May God Almighty bless you all. Thank you so much.

ACKNOWLEDGEMENTS

l would like to take this opportunity to thank the Lord Almighty for his guidance through out the whole program and affording me life to count my success.

I wish to express my profound appreciation to the Commander Zimbabwe National Army, Lieutenant-General PV Sibanda, for affording me the opportunity to fulfill my dream. Sir, you have left an indelible mark in my life and career. I thank you most sincerely. I am also especially indebted to Colonel W Tutisa, Lieutenant-Colonel A Malamo and Major L Msipa for their priceless support, advice and mentoring during this project.

Let me also express my most profound gratitude to my supervisor Mr. Kazembe for his unremitting patience, guidance and mentorship during the course of this dissertation. I enjoyed your wise counsel. May I also acknowledge the support of all the lecturers at Midlands State University, in particular, Mr Mvura (the chairperson), Mr. Mazhindu, Ms. Mhaka, and Ms. Nyamwanza, to mention just a few.

Lastly, I would also like to thank all officers, men and women of the Zimbabwe defence Forces (ZDF) who have assisted me in one way or another during this dissertation. I gratefully count on your invaluable support, because without such support, it would have proved an insurmountable task for me to complete the project. Your cooperation is greatly appreciated. May the great God bless you abundantly.

ABSTRACT

The investigation of the challenges of implementing the RBIA in the ZNA was prompted by the growing calls for effective, efficient and economic utilisation of the finite audit resources to achieve the most impact in terms of IA service. The objectives of the study were to identify the key tenets of a RM framework, determine the role of IA within the risk management (RM) framework, determine the adequacy of the RM framework of the ZNA, identify areas of significant risk, and suggest a RM model that is best suited to address the identified risks.

The study was conducted in the ZNA King George 6 Barracks. A sample of 43 officers from the departments of Finance, Procurement, IT, Pay, Military Police and IA were chosen as respondents using purposive (judgmental) sampling techniques. Thirty-seven self-administered questionnaires and six personal interviews were used to gather data.

Findings from the study revealed that the major challenges were to do with the absence of a documented and approved RM policy in the Army, lack of institutional structures for RM, decentralized RM processes not appropriately embedded within the existing hierarchical structures of the Army, and lack of consciousness on the part of the generality of members within the rank and file of their individual risk responsibilities.

From the study, it was recommended that a RM policy framework be put in place, risk education and training form part of every solder's training syllabi and risk structures be established with clearly defined risk responsibilities. Above all, it was recommended that the AI implements RBIA in order to concentrate effort on areas of heightened risks.

List of Tables

Table Number	Table Name	Page
Table 1.1	Military Offences Set Down by GCM From 2011 to 2013	2
Table 2.1	Risk Management Process	16
Table 2.2	Risk Management and Scoring System	17
Table 3.1	Sample Size in Relation to the Population	26
Table 3.2	Likert Scale	28
Table 4.1	Response Rate From Questionnaires	32
Table 4.2	Tenets of a Risk Management Framework	33
Table 4.3	Role of Internal Audit in Risk Management	34
Table 4.4	Adequacy of RM Framework to Address the ZNA’s Risk Profile	38
Table 4.5	Areas of Significant Risk to the ZNA	41
Table 4.6	Suggested Risk Management Model	44
Table 4.7	Response Rate From Interviews	45

List of Figures

Figure Number	**Figure Name**	**Page**
Figure 4.1	Internal Audit Reviews Risks to Assets and Resources	35
Figure 4.2	IA Identifies Weaknesses and Recommend Improvements	36
Figure 4.3	IA runs Risk Workshops in the ZNA	37
Figure 4.4	Adequacy of Risk Management structures	39
Figure 4.5	RM Framework was Developed to Address Areas of High Risk	40
Figure 4.6	Respondents Views on IT and Pay Directorates	42
Figure 4.7	Respondents Views on Finance and Procurement Directorates	42
Figure 4.8	Respondents Views on Organisation Culture and Governance	43

List of Appendices

Appendix Number	Appendix Name	Page
Appendix 1	Request for Authority to Carry Out Research in the ZNA	56
Appendix 2	Request to Complete Questionnaire	57
Appendix 3	Questionnaire Guide	58
Appendix 4	Interview Guide	63

List of Abbreviations and Acronyms

Abbreviation/Acronym	
PFMA	Public Finance Management Act Chapter 22:19
ERM	Enterprise-wide Risk Management
RM	Risk Management
IIA	Institute of Internal Auditors
CIIA	Chartered Institute of Internal Auditors
COSO	Committee of Sponsoring Organisation of Treadway Commission
RBIA	Risk Based Internal Auditing
ZNA	Zimbabwe National Army
ZDF	Zimbabwe Defence Forces
AIAD	Army Internal Audit Directorate
IA	Internal Audit
Comd ZNA	Commander Zimbabwe National Army

Table of Contents

Content **Page**

Approval Form i

Release Form ii

Dedication iii

Acknowledgements iv

Abstract v

List of Tables vi

List of Figures vii

List of Appendices viii

List of Abbreviation and Acronyms ix

Chapter 1 Introduction

1.0 Introduction 1

1.1 Background of the Study 1

1.2 Research Problem 3

1.3 Research Questions 4

1.4 Research Objectives 4

1.5 Assumptions 4

1.6 Significance of the Study 4

1.7 Delimitations 5

1.8 Limitations 5

1.9 Key terminology 6

1.10 Summary 6

Chapter 2 Literature Review

2.0 Introduction 7

2.1 Tenets of a Risk Management Framework 7

2.2 The Role of IA Within the Risk Management Framework 9

2.3 Risk Management Structures 11

2.4 Areas of Significant Risk 13

2.5 Risk Management Models 15

2.6 Summary 18

Chapter 3 Research Methodology

3.0 Introduction 19

3.1 Research Design 19

3.2 Types of Research Designs 22

3.3 Sampling Techniques and Procedures 25

3.4 Instrument Design: Validity and Reliability 28

3.5 Data Collection, Analysis and Presentation 31

3.6 Summary 31

Chapter 4 Data Presentation, Analysis and Interpretation

4.0 Introduction 32

4.1 Research Findings 32

4.2 Tenets of a Risk Management Framework 33

4.3 The Role of IA in Risk Management 34

4.4 The Adequacy of Risk Management Framework in the ZNA 38

4.5 Areas of Significant Risk to the ZNA 41

4.6 Suggested Risk Management Models 44

4.7 Response Rate From Interviews 45

4.8 Review of Secondary Data 46

4.9 Summary 46

Chapter 5 Summary, Conclusion and Recommendations

5.0 Introduction 48

5.1 Summary of Chapters 48

5.2 Major Findings 49

5.2.1 Tenets of a Risk Management Framework 50

5.2.1 The Role of IA Within the Risk Management Framework 50

5.2.2 Risk Management Structures 50

5.2.3 Adequacy of the RM Framework to Address the ZNA's Risk Profile 51

5.2.4 Areas of Significant Risk to the ZNA 51

5.2.5 Suggested Risk Management Models 51

5.3 Conclusion 52

5.4 Recommendations 52

CHAPTER 1

INTRODUCTION

1.0 Introduction

The first chapter serves to give a general overview of the concept of risk based internal audit (RBIA). It explores the need for a RBIA approach as opposed to the traditional audits of beginning and ending by looking at controls. It further spells out the aim and objectives of the study, assumptions which underpin the research study, its significance, delimitations and limitations, as well as definition of terms which shall be used frequently in the project and summary of the chapter.

1.1 Background

The need to manage risk is increasingly becoming an indispensible part of good corporate governance. Against this backdrop, organisations, both private and public, are under increasing pressure to identify all the inherent risks that they face and direct their energies towards managing these risks. It is the role of management to put in place a sound system of internal control, which in itself, is an essential component of good corporate governance (CIIA, 2014). While it is management's responsibility to identify and manage risk, the internal audit (IA) function is responsible for providing assurance that the risk is being managed properly in the context of the entity's risk management framework. Hence, the IA function must take a risk-based stance in auditing as opposed to the control based approach to auditing (Chinweike, 2012).

RBIA is a contemporary audit approach which is primarily focused on the inherent risks involved in the activities or systems of an entity, and provides assurance that the risks are being managed by the management within the defined risk appetite level. The RBIA methodology recognizes that resources are seldom plentiful, and therefore, the finite resources need to be committed to those areas of significant risk to the entity. The approach is intended to efficiently and effectively focus on the nature, timing and extend of audit procedures to those areas that have the most potential for causing material misstatements (Fraser, 2011).

In the Zimbabwe National Army (ZNA), the Commander is responsible for instituting a sound system of internal control in pursuit of good corporate governance. To this end, the commander is assisted by an IA function as enshrined in the Public Finance Management Act (PFMA) Chapter 22:19 section 80, which requires every state enterprise and parastatal (SEP) to have an IA function integral to its organisation. The IA function assists management in ensuring that there is judicious management of state property against damage, loss, destruction and any other forms of misappropriations.

The Army Internal Audit Directorate (AIAD) is the IA function responsible for providing risk assurance to the commander. Given that the ZNA receives substantial amounts of financial and other resources from the fiscus, and has high value assets in its inventory, the need for a robust risk management plan cannot be overemphasized. A RBIA is therefore inescapable to ensure a dynamic contribution to good corporate governance, sound risk management and more reliable internal controls.

Notwithstanding the presence of a fully fledged IA function, the ZNA has continued to experience a number of criminal cases. For the period from 2011 to 2013, there have been 183 criminal cases that were committed, reported and set down by General Court Martial (GCM) in the ZNA. Table 1.1 is a summary of cases that were committed, reported and tried by GCM during the period under review*:*

Table 1.1: Military Offences Set Down by GCM From 2011 to 2013

Serial	Military Offence	2011	2012	2013	Total
1	Theft of Military Assets	19	23	32	**74**
2	Fraud	7	22	16	**45**
3	Loss of controlled firearms & ammunition	6	5	2	**13**
4	Unlawful possession of drugs	1	5	1	**7**
5	Negligence/destruction of Assets	9	-	9	**18**
6	Diversion of electricity	-	-	1	**1**
7	Bribery/ Forgery	-	4	5	**9**
8	Criminal abuse of office	-	15	10	**25**
	Total	**42**	**74**	**67**	**183**

Source: Directorate of Prosecutions (ZDF HQ) Annual Reports as at 10 July 2014

Theft cases increased by 21% in 2010 and by a further 39% in 2013. The theft of 20 AK 47 rifles from Pomona Barracks armoury in 2010, coupled with cases involving unlawful possession of ammunition and firearms, possesses a serious security risk of armed robberies and acts of banditry in the country. Fraud cases increased by 214% from 2009 to 2010 before dipping by 27% in 2013. During the period November 2013 to January 2014, a computer programmer in the IT Department criminally manipulated a computer program to defraud every member of the force of $2,00 from every member's salary (Special Investigations Branch Docket Number 78/14 dated 15 January 2014). Given the ZNA's manning levels of over 35,000 members, the amount of prejudice is about $210,000 over the period. A case of such a magnitude reflects the high level of vulnerability of the ZNA to the risk of cyber crime.

It should also be noted that not all military offenses are brought to the GCM for trial. Instead, the GCM is the highest military court which tries cases above a certain magnitude and threshold in terms of prejudice to the state. Other cases below this threshold are dealt with and disposed of by lower military courts through summary trial. Hence, the above statistics are only indicative of offenses that warranted being set down by GCM. It is therefore apparent that the ZNA suffer significant risks which require a RBIA approach so that the risks can be reduced to acceptable levels.

1.2 Research Problem

The AIAD plays a pivotal role of providing risk assessment, control assurance and compliance work in furtherance of the governance structures of the ZNA. However, the ZNA has continued to experience criminal cases despite having an IA function. The IA utilizes the traditional control based auditing approach which has so far failed to reduce risk to acceptable levels. This approach has failed to prevent, detect and correct internal control weaknesses that are prevalent in the organisation as evidenced by the high number of criminal cases that have been reported, tried and set down. As such, the research seeks to investigate the challenges of utilizing the RBIA approach in the ZNA to reinforce the responsibility of management for managing risk.

1.3 Research Questions

- What are the tenets of a credible risk management framework?

- What is the role of the IA within the risk management structure?
- To what extend is the risk management framework adequate to address the ZNA's risk profile?
- What are the areas of significant risk to the ZNA?
- Which audit responses are appropriate to address the identified risks?

1.4 Research Objectives

- To identify the key tenets of a risk management framework.
- To determine the role of IA within the risk management framework.
- To determine the adequacy of the risk management framework of the ZNA.
- To identify areas of significant risk.
- To suggest a risk model or approach that is best suited to address the identified risks.

1.5 Assumptions

- All information obtained from respondents is accurate, reliable, true, fair and unbiased.

- The sample selected is a true representative of the total population concerning the results of the study undertaken.

- The current traditional compliance-based internal auditing approach will not change at least within the foreseeable future.

1.6 Significance of the Study

1.6.1 To the Student

The research is done in partial fulfilment of the Bachelor of Commerce Honours Accounting Degree at the Midlands State University.

1.6.2 To the University

The research may provide a source for further research by other students who may have an interest in this area of research.

1.6.3 To the Organisation

The ZNA will benefit from some of the recommendations proffered by the researcher. In particular, it will lead to the following:

- The re-orientation of the IA to conduct their audits from a risk-based perspective as opposed to the traditional control-based audit.
- The achievement of efficiency, effectiveness and economic utilization of the finite resources by concentrating effort on areas of heightened risk.

1.7 Delimitations

The research is limited to investigating the challenges of utilizing the concept of RBIA in the ZNA. Furthermore, as time and other resources are never adequate for such a research, the researcher covered period from 1 January 2009 to 31 December 2013, and will target respondents located in and within the environs of Harare.

1.8 Limitations

1.8.1 Confidentiality

The military profession is a discipline that upholds highest standards of confidentiality. As such, information could not be easily disclosed. Some information had to be censored before the researcher was allowed to include it in the research. To go around this challenge, the researcher gave respondents assurances that the information and the resultant findings were required purely for academic purposes. In addition, the researcher employed the process of triangulation in order to achieve synergy.

1.8.2 Time Constraints

The time allocated for the research was just about two months and it was difficult to reach out to some of the respondents deployed in military establishments outside of Harare. Against this background, the researcher placed reliance on telephone interviews, questionnaires and emails to reach many respondents.

1.9 Key Terminology

1) Internal Audit – is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes (IIA, 2004).

2) Enterprise-wide Risk Management (ERM) – a structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives (IIA, 2004).

3) Risk – the potential of losing something of value which hinders the achievement of objectives (Griffiths, 2013).

4) Risk Appetite – the amount of risk that an entity is willing to accept within its overall capacity. It is the threshold of acceptable risk (Griffiths, 2013).

1.10 Summary

The first chapter highlighted the background of the problem, statement of the problem, research questions, research objectives, assumptions, the significance of the study, delimitations and limitations of the study. Chapter 2 intends to review the related literature in order to answer the research questions and objectives.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

The second chapter reviews literature from secondary sources such as books, journals, magazines and other reputable authorities that have contributed research towards the area of RBIA. This review of relevant literature is necessary in order to answer the research questions and thus achieve the research objectives. In this chapter, literature relevant to each objective will be considered and reviewed in turn. This will assist the researcher in the investigation of the challenges of implementing a RBIA approach in the ZNA and ends with a summary.

2.1 Tenets of a Risk Management Framework

Griffiths (2013) defines RBIA as "the methodology that provides assurance that the risk management (RM) framework is operating as required by the board." It follows therefore from this definition that a RM framework is the precursor of RBIA. RM itself is defined by Miksen (2014) as "the practice of identifying potential risks in advance, analyzing them and taking precautionary steps to reduce or curb the risk." The pertinent steps of a RM process are captured in the definition provided by the Business Dictionary which defines risk management as "the identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks" (http://www.businessdictionary.com/definition/risk-management.html: 21 August 2014 at 15:45 hours).

The Committee of Sponsoring Organisations of Treadway Commission (COSO, 2004) cited in Fraser and Henry (2007:393) defines Enterprise-wide Risk Management (ERM) as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives". According to Griffiths (2013:7), RBIA as an internal auditing approach that provides an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels. Griffiths cited in Castanheira, Rodrigues and Craig (2010:80) state that RBIA focuses on areas of heightened risk and conducts continuous assessments of risk. They believe the work of IA has shifted focus from control-driven to being business risk-driven.

It is clear from the COSO's definition that responsibility for ERM lies with an entity's board and management, and that ERM cuts across the entire entity in order to facilitate the achievement of an entity's objectives. Responsibility for ERM is also apportioned to 'other personnel' in this definition. This could be a specifically established unit, such as a risk management unit or an audit committee, or it may refer to an IA function which is mandated to be in charge of ERM or its assurance thereof. Being a process, ERM involves some steps which have been highlighted in this defining and on the definition that was proffered by the IIA (2004), which include among others, identifying risk, assessing risk and deciding on responses.

The Turnbull Review Group (FRC, 2005) has played a pivotal role in inspiring recent developments in RM. As a consequent of increasing pressure on corporate boards to report on the effectiveness of RM and internal control, the Turnbull came up with overwhelming recommendations that have significantly contributed to the overall improvements of the standards of RM and internal control (Fraser and Henry, 2007:394). The Turnbull advocated for boards to adopt risk-based approaches to internal control and to subsequently monitor their effectiveness. This was against the background that companies tended to concentrate on only financial risk yet a comprehensive risk assessment considers all the risk factors that an entity faces which include financial, business, compliance, operational and any other risks (Fraser and Henry, 2007:392-3).

According to Griffiths (2013), the structures in a RBIA include the various stakeholders, the board, an audit committee, management, risk manager, IA and every employee.

The stakeholders have entrusted their stake on a board and thus expect the board to deliver the long-term success of the entity. On its part, the board sets a risk appetite which should guide management in its implementation of internal controls to manage risk to levels that the board considers acceptable. In order to ensure independence and objectivity, an IA function has a strong reporting line to an audit committee. The primary responsibility of an IA being that of providing an independent and objective opinion to management on whether the entity's risks are being managed to acceptable levels. Management on their part, are assisted in the identification, assessment and management of risk by a risk manager.

Little (2013) cited in Schroeder (2014:29) believes that RM is no longer a distinct area of business management which can be performed by a single person or unit. Instead, it requires that every employee is risk-conscious and must take a proactive stance in managing risk in their day to day work. However, this does not discount the key role that leadership and management, and the support of organisation systems play in helping employees acquire the necessary skills and attitudes to identify and manage risk.

2.2 The Role IA Within the Risk Management Framework

The IIA (2009) cited in Castanheira, Rodrigues and Craig (2010:82) assert that, upon request, an IA can assist in the initial establishment of a RM framework in an organisation that does not have one. This task fits in well with the IA's consultancy role in the quest of improving an entity's fundamental processes.

According to Griffiths (2013:2), management is responsible for the following duties in pursuit of the goal to achieve the objectives of an organisation; identifying risk; ranking and scoring the risk; receiving from the board their risk appetite; implementing internal controls to bring risk to levels below the board's risk appetite; and assuring the board that it is monitoring internal controls so that risk remains below the risk appetite.

Within this responsibility setup, Griffiths (2013:4) states that the main aim of an IA is to assist an organisation achieve its objectives. He asserts that the IA function achieves this mandate by 'providing an independent and objective opinion to an organisation's management as to whether its risks are being managed to acceptable levels.' In Griffiths' view, this mandate of the IA is the definition of risk based internal auditing. Hence, the objective of an IA is to tell management and through them stakeholders, whether risks are being managed properly. Given that internal controls are processes designed to manage risk to levels below the entity's risk appetite, an IA must therefore know this risk appetite, against which the significance of risks can then be measured. It is the duty of the board to define the risk appetite. Both management and IA must have a common understanding of this threshold of risk appetite and accept it as given. The board itself is responsible to stakeholders to ensure compliance with legislation which require it to maintain a proper system of internal control.

Despite an entity having a risk manager, the accountability of management for identifying and managing risk cannot be delegated. Instead, risk managers assist the organisation in identifying risk, running risk workshops, coaching staff in risk management and setting 'best practice standards' (Griffiths, 2013:5). Against this background, the responsibility of an IA remains that of providing advice in the form of an opinion on whether the entity's risks are being managed within acceptable levels.

The IIA cited in Fraser and Henry (2007:396) defines the primary roles of an IA concerning ERM as "providing objective assurance to boards that the principal business risks are being managed appropriately and that the internal control framework is functioning effectively". To be able to provide an objective assurance, the IA function must be separate from the risk management process, but should be allowed uninterrupted opportunity to comment on the appropriateness of risk management and internal controls. Such a scenario entails therefore that the depth of IA understanding of risk management must be beyond reproach. Where the IA lacks appropriate skills, it is suggested that an entity outsources in whole or in part in order to bring in specialist skills. This is particularly true given the traditional IA departments which mainly comprise personnel from financial backgrounds.

Griffiths believes that the identification of risks by management is the single most important part of a RBIA. This process (of identifying risks) is followed by the responses that management puts in place to mitigate the effects of the potential risks identified. Based on these, the IA's principal responsibility is that of providing an opinion on whether risks are being managed to acceptable levels. It therefore follows that the IA must have a sound appreciation of the established system of measuring risk, the defined risk appetite, and the framework for categorizing, recording and ranking (or scoring) the inherent risks.

It is now established that management must identify, score and manage risks, and give the comprehensive list of risks to the IA department. On the basis of this list, the IA must then design an audit plan of work in order to deliver on its mandate. Although the IA may also assist in identifying risks, it cannot take part in the management of risks since doing so would affect their objectivity (Griffiths, 2013:7).

2.3 Risk Management Structures

Schroeder (2014:29) believes that every employee must play a part in risk management. This, however, does not discount the need to appoint a risk manager who would ensure that risk management is properly integrated into the business strategy. The IIA as cited in Fraser and Henry (2007) recognises different structures that are charged with specific responsibilities within the risk management framework of an entity. The various stakeholders expect the board to deliver the long term success of the entity, observe the dictates of all relevant legislation and institute a proper system of internal control. The board sets its risk appetite and demand management to contain risk within the risk appetite. Management on their part, possibly with the assistance of a risk manager, will put in place a risk management framework and implement internal controls to manage risk (Griffiths, 2013). Within this framework, the IA gives their independent and objective opinion on whether the entity's risks are being managed to acceptable levels (Griffiths, 2013; Castanheira, Rodrigues and Craig, 2010; Tummala and Schoenherr, 2007).

Section 80 of the Public Finance Management Act (PFMA) Chapter 22:19 provide for the establishment of an IA function integral to any state enterprise, public entity or parastatal. The same section sets out the duties of the person so appointed as internal auditor, their rights and reporting channels. The Internal Auditor is responsible for assessing the cost-effectiveness of any projects undertaken by the Ministry or reporting unit concerned. He/she is also responsible for monitoring the financial administration and procedures of the Ministry or reporting unit concerned. In particular, he/she should ensure that proper accounting and bookkeeping transactions and procedures are carried out; proper accounting records are maintained; adequate internal checks and controls are observed; assets under the control of the reporting unit are properly accounted for; and instructions and directions issued in terms of the PFMA are complied with.

These duties tend to incline an IA function to institute a traditional control-driven auditing approach as opposed to a risk-driven auditing approach. This is because the duties are compliance biased and hence predisposes and canalizes the IA function to give an opinion on compliance rather than giving it the latitude to formulate its audit strategy and programme based on the assessed areas of significant risk.

Section 84 of the same Act provides for an audit committee, its duties and privileges. The audit committee is responsible for reviewing internal controls, including the scope of the internal audit programme, the internal audit findings, and to recommend appropriate action to be taken by the responsible authorities, among other duties. These duties impose on an audit committee, an important responsibility as regards risk management. The same section spells out the qualifying criteria for persons who should hold portfolios in the audit committee. This criteria conforms with the provisions of the King III Report (2009), which require that members sitting on the audit committee be independent non-executive directors.

Section 81 of the PFMA provides that the Auditor-General shall audit or cause to be audited the financial statements of annual appropriations of the Consolidated Revenue Fund, all other public funds, public entities and constitutional entities. The Act requires the Auditor-General to satisfy himself or herself that all reasonable precautions have been taken to safeguard the collection of public money and that the provisions of this Act and any other enactment relating to the accounting for public resources and of any direction or instruction issued have been duly observed. Among other duties, the Auditor-General shall ensure that all reasonable precautions have been taken to safeguard and control State property and all issues of State property are made in accordance with proper authority. These duties have a direct and an invaluable contribution towards the risk management efforts of any state enterprise, public entity or parastatal.

Section 5 of the Audit Office Act Chapter 22:18 gives the outline duties of the Auditor General. The Auditor-General is responsible for, on behalf of Parliament, auditing the accounts of any public entity, or designated corporate body. The Auditor General may also carry out examinations into the economy, efficiency and effectiveness with which any Ministry, public entity, local authority or designated corporate body, statutory fund or other body which has used public resources in discharging its functions. Section 7 of the Act requires the Auditor-General to satisfy himself or herself that public moneys and State property are safeguarded. In performing these duties, the Auditor General becomes a critical player in the risk management structures of public entities.

2.4 Areas of Significant Risk

King III Report (2009) recognises that the economic value of a company can no longer be judged by financial criteria alone, but rather, other non-financial factors such as quality of governance, reputation, stakeholder relations, social responsibility, etc. Consequently, the King report identified key governance elements that have a direct impact on the overall corporate governance framework of any entity which include IT governance, risk governance, internal control, sustainability and going concern, efficient and effective use of resources, payroll issues, among others.

Rubino and Vitalla (2013:324) contend that the use of IT in business has brought with it some benefits and costs in pursuit of the achievement of entity objectives. IT has helped a great deal in the management of information, improvement of business processes, aiding decision-making and performance measurement. However, there are challenges that management have to organise the delivery of IT services, monitor the quality level of information services and align IT resources with the entity's processes and the business activities. Pramod, Li and Gao (2012:172) argue that, despite the level of sophistication, the need for human intervention to make decisive judgments about system outputs, is inevitable.

Schroeder (2014:28) gives insight into what constitute areas of significant business risk when he intimated that the biggest catalyst in all areas of business is ultimately determined by the actions of people. He cited difficulties in changing employee attitudes and behaviors, weak leadership, stakeholder resistance, or poor communications as some of the common factors behind businesses failures.

According to Schroeder (2014:29), corporate culture is one of the biggest risks that organisations face in the contemporary business environment. He believes that culture influences behaviors and attitudes that tend to "reinforce old ways of doing things at work" and this could prove counter-productive to implementing new corporate strategy. Schroeder suggests that there should be effective employee engagement in order to manage change and so bring about new cultural norms. To develop a new culture that dovetail the new strategy, Schroeder identifies compensation, benefits, reward system, organisational structure, and leadership system as "change shaping levers". He asserts these levers are key in rewarding or penalizing employees for exhibiting certain behaviors or attitudes.

In his 2014 National Budget Statement, the Minister of Finance Mr. P Chinamasa (2013:115-118) underscored the need to strengthen governance and accountability in public resource management. The Minister noted the glaring shortcomings in the public procurement systems and suggested revamping the arrangements and processes to achieve efficiency, transparency, accountability and professionalism.

2.5 Risk Management Models

In a bid to propose comprehensive and coherent risk management approaches, a number of authorities have put forward risk management models that are designed to manage risk in various business environments. The prominent risk management proponents as cited in Tummala and Schoenherr (2013:475) include Tummala et al (1994), Zsidisin and Ellram (2003), Kilgore (2004), Kleindorfer and van Wassenhove (2004), Sinha et al (2004), Kliendorfer and Saad (2005), De Waart (2006), Manuj and Mentzer (2008), Schoenherr et al (2008), Ellegaard (2008), and Griffiths (2013).

Tummala *et al* cited by Tummala and Schoenherr (2011:475) formulated a risk management approach called risk management process (RMP). They identified five phases of the RMP, which are; risk identification, risk measurement, risk assessment, risk evaluation and risk control and monitoring. Tummala and Schoenherr (2011:475) then modified and extended the works of Tummala *et al* (1994) by collapsing the five phases into three phases but with six steps in a risk model they called Supply Chain Risk Management Process (SCRMP). They identified the first phase as comprising the steps of risk identification, risk measurement and risk assessment. The second phase include two steps of risk evaluation, and risk mitigation and contingency plans, while the third phase involves a single step of risk control and monitoring. In essence, Tummala and Schoenherr presents a conceptual framework and approach that is applicable in supply chain settings by adding only the step of risk mitigation and contingency plans on the phases proposed by Tummala et al (1994).

According to Tummala and Schoenherr (2011:476), risk identification involves determining all the potential risks associated with a given problem and also identifying the areas that are likely to be affected and the resultant consequences. This allows for the formulation of strategies in order to mitigate the effects of the risk on the areas which are likely to be affected. The two assert that it is important to start by listing all the possible threats, and for each threat, identify the resources (assets, people or earnings) of the entity that could be affected. Thereafter, formulate the responses that are appropriate to mitigate the effects on the entity's achievement of objectives.

Risk measurement involves the determination of the extend to which the threats manifests its effects upon the resources (i.e. the consequences). Tummala and Schoenherr (2011:476) claim that manifestation may include loss of or damage to assets, loss of income, interruption of service, poor process performance, injuries, etc. They classified risk in terms of four attributes and the following matrix can be derived to depict the classification of risk in terms of consequence, frequency, severity and predictability:

Table 2.1 Risk Management Process

Undesirable consequences	**Frequency**	**Severity**	**Predictability**
Trivial	Very high	Very low	Very high
Small	High	Low	Reasonable
Medium	Low	Medium	Reasonable
Large	Very low	High	Minimal

Source: Tummala and Schoenherr (2011:476)

Trivial and small losses are expected to occur in an organisation as they represent little problems unless if their frequency becomes high that when aggregated they reach the threshold of medium losses. Medium losses, although not preferred, would not cause serious concerns for the entity as these could be expressed as annual amounts in the form of provisions. However, large losses represent the significant losses that are of great concern to the entity. These kinds of losses are rare, but should they occur, they could cause grievous harm to the entity.

Griffiths (2013:10) suggests a simple and effective risk measurement method which considers only two characteristics; consequence when risk occurs and likelihood (probability) of risk occurring. These two characteristics are given different scores ranging from one to five so that if the consequence and the probability are multiplied together using different combinations of scores, they give a single measure of the significance of a risk. Table below illustrates the risk measurement and scoring system proposed by Griffiths:

Table 2.2 Risk Measurement and Scoring System

Consequence		**Probability**	
Magnitude of Consequence	**Score**	**Probability**	**Score**
Close down the entity, or a significant part, for a long time.	Very high (5)	Almost certain	Very high (5)
Prevent the entity achieve a major part of its objectives for a long time.	High (4)	Probable	High (4)
Stop the entity achieve some of its objectives for a limited time.	Medium (3)	Possible	Medium (3)
Cause inconvenience but not affecting the achievement of significant objectives.	Low (2)	Unlikely	Low (2)
Cause very minor inconvenience but not affecting the achievement of objectives.	Very low (1)	Rare	Very low (1)

Source: Griffiths (2013:10), [Available: www.internalaudit.biz: Accessed 21 July 2014 at 15:23 hours].

Risk assessment is concerned with the assessment of uncertainties and determining the likelihood of each risk factor occurring. This assessment utilises probability distributions using the conventional techniques such as the Delphi method, expert focus groups, parameter estimation, etc (Tummala and Schoenherr, 2011:478). According to Fraser and Henry (2007:394), the assessment of risk requires all stakeholders in the entity's hierarchy by adopting a "bottom up" approach. This allows for the work of junior risk identification teams to have their work evaluated by more seniors teams and thus facilitate a common understanding and approach to risk management.

Risk evaluation is concerned with the ranking of risk and determining the threshold of acceptable risk (i.e. the risk appetite). It is at this stage that cross-functional teams and senior management work together to agree on the risk threshold and categorises risk into a hierarchy of acceptable, tolerable and unacceptable risk. Griffiths (2013:8) concurs with Tummala and Schoenherr on the idea of categorizing risks into this kind of hierarchy. The fifth step is risk mitigation and contingency plans which is concerned with the development of risk responses to contain and control the risk.

The last step is risk control and monitoring. It involves continuous monitoring of the implemented risk responses, and where necessary, take corrective action to ensure that the risk responses are efficient and effective. There is also need for continuous monitoring and assessment of the risk responses in order to improve the risk management process itself.

2.6 Summary

The chapter sought to provide a theoretical base for the research. It has highlighted the tenets of a sound risk management framework, the role of IA in risk management, risk management framework in organisations, gave a synopsis of available risk models, and determined the significant risk the organisations face and suggest appropriate responses to mitigate these risks. Chapter 3 intends to outline the research methodology that was used to gather evidence in order to answer the research questions and objectives.

CHAPTER 3

RESEARCH METHODOLOGY

3.0 Introduction

This chapter gives a detailed description of the methodology that the researcher used to gather data and other evidence essential in order to satisfy the research objectives. It also examines the various types of research designs, and the justifications for the choice of research design that the researcher considered feasible and appropriate to the research. The chapter is also concerned with the determination of the population, sample size as well as the sampling techniques utilised to collect data. Lastly, it considers data collection instrument design in terms of validity and reliability, and ends with a summary.

3.1 Research Design

Vaccaro (2014) defines research methodology as a collective term used to describe the structured process of conducting research. He asserts that the key components of research methodology include research design, data gathering and data analysis (http://science.blurtit.com/23704/what-is-research-methodology-: Accessed on 8 September 2014 at 15:22 hours). Simply put, research methodology is the general outline guiding the research project. The Business Dictionary defines research design "as a detailed outline of how an investigation will take place. A research design typically include how data is to be collected, what instruments will be employed, how the instruments will be used and the intended means for analyzing data collected" (http://www.businessdictionary.com/definition/research-design.html: Accessed on 8 September 2014 at 14:07 hours). The chosen research design must be used as a guide in gathering and evaluating data in order to answer a particular research objective.

Basically there are two categories of research designs which are; the quantitative method and the qualitative method. Quantitative research is a systematic method that utilises numbers, tables, graphs and charts to depict numerical data. On the other hand, qualitative research is a subjective and descriptive method which is concerned with non-quantifiable elements such as feelings, opinions, attitudes, behaviours, etc (Denscombe, 2010 and Jackson, 2011). Ideally, a comprehensive research must try to incorporate both quantitative and qualitative methodologies but this may not always be possible owing to constraints of time and other resources (e.g. financial resources).

3.1.1 Quantitative Research

Quantitative research methods utilise numerical data to describe a phenomenon (VanderStroep et al, 2010; Denscombe, 2010 and Jackson, 2011). It is possible to measure the frequency of occurrence on the basis of numbers, and present such information in the form of tables, graphs, charts and frequency distributions (Walliman and Walliman, 2011:7). It also allows for scope to inquire specific questions from the respondents and the results can be codified as statistics which provide some degree of certainty. The research procedures tend to be standard and can be replicated for other studies (Jackson, 2011; and Denscombe, 2010).

The most popular types of research methods in this category include; closed-ended questionnaires, experiments, surveys, correlation and regression analysis methods, mean, mode and median and others (Cohen et al, 2007; Jackson, 2011; VanderStroep et al, 2010 and Denscombe, 2010). During the research, the questionnaire and the mode will be used. The questionnaire allows the researcher to reach out to a number of respondents while the mode allows the research to determine the response with highest frequency among respondents.

3.1.1.1 Justifications

VanderStroep et al (2010) allude to the ability for quantitative research to provide for statistical validity as its major strength. The usually large sample size allows the research to be accurately reflective and representative of the population. Ledgerwood and White (2006) assert that a quantitative research is conclusive in that its results can be inferred to the rest of the population. They argue that this category of research allows for the measurement of the degree and frequency of phenomena.

However, according to VanderStroep et al (2010), the primary disadvantage of quantitative research is that it allows for only superficial understanding of participants' thoughts and feelings. Ledgerwood and White (2006) affirm that quantitative research can be costly and time consuming, and also that the questionnaire can be biased in its form and content.

3.1.2 Qualitative Research

Qualitative research methods utilise a narrative fashion to describe a phenomenon. The scope of its analysis is to identify major schemes and broad thematic concerns. Denscombe (2010) claim that procedures in qualitative researches are unique for each study and usually cannot be replicated. The research is intended to provide an in-depth understanding of the phenomenon.

The most popular types of research methods in this category include; open-ended questionnaires, interviews, focus groups, case studies, observation, gamming and role playing, among others. During the study, the research will make use of the interview and the case study research methods.

3.1.2.1 Justifications

VanderStroep et al (2010) state that the major strength of qualitative research lies in its ability to provide for a rich and in-depth narrative description of the sample. The research is interpretive in nature and seeks to unpack the underlying behaviours.

According to VanderStroep et al (2010), the primary disadvantage of qualitative research is that it uses a small sample which is difficult to generalize to the rest of the population. Ledgerwood and White (2006) affirm that qualitative research is subjective and biases can be introduced in the execution and analysis of results.

To go round the challenges highlighted on the two categories of research designs, the researcher adopted what can be referred to as the ‘mixed research method’ which combines the quantitative and qualitative forms of research in order to make the overall strength of the study greater than either of the two methods (VanderStroep and Johnson, 2010).

3.2 Types of Research Designs

Whilst research designs fall into the two broad categories of quantitative and qualitative research, there are quite a number of types of research designs which are widely used in practice to collect data. The most widely used research designs and the accompanying justifications are explained hereunder:

3.2.1 Explanatory Research

Explanatory research design is research conducted in order to explain any behaviour in the market. It focuses on the rationale behind a phenomenon. In other words, it focuses on ‘why” questions, thus seek to establish the reason why. It could be done using questionnaires, group discussions, interviews, random sampling, etc (Cohen et al, 2007 and Yamagata-Lynch, 2010).

3.2.1.1 Justifications

It is not enough to explain the reasons why military offences have been steadily increasing despite the implementation of routine internal audits, but rather, it is important to examine the challenges of implementing a contemporary internal audit approach to manage the inherent risks in the organisation. This research method would not be used as the researcher does not merely seek to highlighting the reasons for a phenomenon but to go beyond the rationale of establishing an IA approach that manages the organisation’s risks to acceptable levels.

3.2.2 Case Study

The case study research design is increasingly becoming a very useful and popular tool for investigating trends and specific situations in the field of research (Jackson, 2011). A case study is an analysis of persons, events, decisions, periods, projects, policies, institutions or other systems that are studied holistically by one or more methods (Thomas, 2011:511). It involves descriptive, exploratory or explanatory analysis of a person, group or event.

A case study helps a researcher to understand complex issues and in extending experience and strength to what is already known by asking questions which begin with "how" or "why" (Yin, 2011). This is quite critical in giving insights into how and why a contemporary phenomenon under study is what it is.

3.2.2.1 Justifications

Yin (2011) affirm that case studies allow for rich data to be collected that provides greater depth than other research designs. A case study also tends to be conducted on rare cases where large samples of similar participants are not normally available. Its major shortcomings are that the data collected cannot necessarily be generalized to the wider population, it is not scientific and cannot be definite in establishing a cause-and-effect relationship.

The researcher would make use of the case study since it is ideal for investigation of contemporary phenomena. The research design also provides rich data quality which is insightful for greater understanding of the underlying concepts of the research problem. The RBIA is a contemporary internal auditing approach that can benefit the ZNA in reducing its risks to acceptable levels.

3.2.3 Descriptive Research

Descriptive research is used when researchers are interested in understanding the opinion of a large group of people about a particular topic or issue. It attempts to describe and explain conditions of the present by using many respondents. It is a quantitative research method that can make use of closed-ended questionnaires to fully describe a phenomenon. This type of research design is commonly used by social researchers to describe human behaviours, by market analysts to describe the habits of customers and to indicate a variable that might be worth testing quantitatively.

In this type of research, researchers ask a number of questions, all of which relate to the issue under study, and collate the answers to determine the general trends, attitudes or opinions of the population using statistical analysis. According to Fraenkel and Wallen (2006), this research method is also known as a 'survey' and might take a variety of forms such as face-to-face, mail or telephone interviews with individual groups. Against this backdrop, the survey research thrives on carefully designed and unambiguous questions, and on the collation and analysis of the answers to determine the trend.

3.2.3.1 Justification

The type of research design employed in this research is the descriptive research. This method allows the researcher the opportunity to reach out to a large group of respondents. Consequently, it will be possible to conclusively draw valid conclusions about the phenomenon given that the large sample might be accurately representative of the entire population.

It is against this background that the survey research would be used to gather data and information that would determine the challenges of implementing a RBIA approach in the ZNA. The major strength of this method, according to Bryman and Bell (2005:5); Ledgerwood and White (2006); Cohen et al (2007); and VanderStroep et al (2010), is that it generates numerical data that can be subjected to statistical analysis, and provide conclusive descriptive and inferential interpretations to the population at large.

Notwithstanding the highlighted advantages, the survey method has its fair share of weaknesses. According to Ledgerwood and White (2006), Cohen et al (2007), and VanderStroep et al (2010), the survey method is costly (e.g. it frequently entails travelling costs) and time consuming. On the other hand, the questionnaire method requires time and costs for construction, plotting, printing, posting, coding, etc. It is also almost certain that some questionnaires may not be responded to, and this impacts negatively on the quality of the analysis and the resultant conclusions.

To mitigate the impact of the aforesaid challenges, the researcher resorted to utilizing telephone interviews, direct administration of the questionnaire to the target group and maximum utilization of electronic mails to sent questionnaires to respondents located in distant places. These measures almost assured the researcher a 100% response rate.

3.3 Sampling Techniques and Procedures

Proctor (2003:100) defines a sample as "some portion of a population." Since a target population would generally have too many subjects to realistically work with directly, some sampling techniques have to be devised to select a sample that is truly representative of the entire population from the large population. Sampling is therefore the specific principle used for selecting members of the population that are to be used in the study. According to Saunders et al (2007) sampling is one of the most critical components of research that involves the collection of primary data from the population. As such, it is important that a researcher selects a sample that is representative, logical and statistically defensible.

3.3.1 Probability Sampling Method

According to Wilson (2010), there are two broad categories of sampling methods, which are the probability and the non-probability techniques. The probability sampling method involves the selection of a 'random sample' from all the members which constitute the population. This method entails that there is an equal chance of any member of the population being chosen, that is to say, the probability is nether zero nor one, but gravitates between zero and one. The popular sampling methods in this category include simple, stratified and systematic random sampling methods.

However, this method of sampling will not be utilised because the researcher intends to collect data from respondents who possess specific characteristics, attitudes, skills and knowledge about the area under study.

3.3.2 Non-Probability Sampling Method

On the other hand, the non-probability sampling technique involves the selection of the population members on the basis of a specific non-random technique. Popular probability sampling methods in this category include snowball, convenience, quota and purposive (judgmental) sampling methods.

In this research, the researcher has purposively selected five officers from each of the following departments; Finance, Procurement, IT and Military Police, eight audit team leaders were selected from the fifteen teams, eight officers from Pay, the chief internal auditor and Chief of Staff Administration Staff to constitute the sample size of the research. Therefore, the thirty-seven members of the sample became the subjects to which the data collection instruments were to be administered. Table 3.1 below illustrates the percentage of the sample in relation to the population:

Table 3.1 Sample Size in Relation to the Population

Department	**Population**	**Sample**	**Percentage**
Finance	9	5	55.5%
IT Directorate	8	5	62.5%
Military Police	10	5	50%
Procurement	9	5	55.5%
Pay	15	8	53.3%
Internal Audit	15	8	53.3%
Total	**66**	**37**	**56.06%**

3.3.2.1 Purposive Sampling Method

Purposive sampling techniques is also variously referred to as judgmental, selective or subjective sampling. According to Patton (2002:237) cited in the Lund Research Ltd (2012) and Robinson (2014), purposive sampling is a subjective non-probability sampling technique that relies on the judgment of the researcher for the selection of subjects for investigating. The technique is usually used to investigate small sample sizes as it focuses on particular characteristics of the population of interest, which is better placed to answer the research questions. There are many types of purposive sampling techniques but the researcher will restrict himself to two types, which are; the heterogeneous and the homogeneous sampling methods.

3.3.2.1.1 Heterogeneous Sampling Method

According to Robinson (2014), heterogeneous (or maximum variation) sampling method is used to capture a wide range of perspectives relating to the issue under study. Its objective is to search for variations in perspectives that range from the typical to the more extreme perspectives. The basic principle behind this method is to gain greater insights into a phenomenon by looking at it from all angles, and so identify common themes that are evident across the sample. The researcher will utilise the Likert scale to get these perspectives from the sample demarcated earlier on.

3.3.2.1.2 Homogeneous Sampling Method

Ribinson (2014) affirms that homogeneous sampling method identifies a sample whose respondents share the same characteristics or traits (e.g. in terms of age, occupation, background, gender, etc). This method is used to examine in detail research questions that address specific characteristics of the particular group of interest. In this regard, the researcher seeks to administer questionnaires that seek to elicit specific perspectives peculiar to IT, Finance, Procurement, Internal Audit and Pay Directorates.

3.3.2.2 Likert Scale

A Likert Scale is one of the range of scale types that researchers can use to provide answers to the research questions by providing a choice from a given range of answers (Rattray and Jones, 2007 and de Winter and Dodou, 2012:3). The scale provide respondents with a range of alternatives in the form of multiple choice answers.

The Likert scale is shown at Table 3.2 below:

Table 3.2: Likert Scale

Item	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
Points	5	4	3	2	1

Source: Burns (2008:474)

3.3.2.2.1 Justifications

The scaling techniques is easy to prepare, easy to read and complete for participants, produces homogeneous scales and increases the probability that a unitary attitude is measured thereby increasing validity and reliability. However, Bertram (2009) criticized the scale for its biases as participants may avoid extreme responses, may agree with statements to 'please' the researcher, may portray themselves in socially favourable light than being honest in their responses. He further states that the scale cannot be reproduced by a different researcher on the same problem and its validity may be difficult to demonstrate as the researcher may fail to measure what he/she set out to measure.

3.4 Instrument Design: Validity and Reliability

3.4.1 Instrument Design

Pierce (2009) defines a research instrument as a survey, questionnaire, test, scale, rating, or tool designed to measure the variable(s), characteristic(s), or information of interest, often a behavioral or psychological characteristic. Questionnaires, interviews, phone surveys and observations are the major tools available for descriptive researches.

In this research, the questionnaire was the main instrument used for data collection. However, the researcher utilised the interview guide to source data from some of the respondents. The questionnaire was used extensively as the major instrument of data collection because it allows the researcher to reach out to a large number of respondents without expending a lot of resources in terms of time and other costs.

However, the questionnaire technique has its own challenges which include low response rate, non-response, misinterpretation of questions and that the questions may be filled without paying due attention to the significance of the study. To address these limitations, the researcher made every effort to visit each respondent to physically administer the questionnaire, and where possible, made prior phone calls to explain the significance of the study to each respondent.

3.4.2 Validity and Reliability of the Instrument

According to Fraenkel and Wallen (2006), validity is the extend to which results from a chosen research instrument permit the researcher to draw warranted conclusions about the characteristics of the individuals studied. They further define reliability as the ability of the research instrument to give consistent results. In other words, reliability is when a research instrument is applied repeatedly to the same object under similar conditions but continues to yield the same result each time.

To ensure validity and reliability, the researcher formulated questions that would adequately and exhaustively address each of the research objectives. It was also incumbent that the researcher took into consideration the appropriateness of the timing, venue, privacy and confidentiality so that respondents would give their honest report of information without any distractions or interferences.

3.4.3 Types of Questions

As has already been alluded to, the researcher can either ask open-ended or closed-ended questions. Where open-ended questions are asked, the respondents provide their individual answers to the questions. In the case of closed-ended questions, respondents are forced to select their answers from a list provided by the researcher. The questionnaires can take a variety of formats such as the dichotomous, multiple choice, rank ordering and rating scales (Cohen, Manion and Morrison, 2013). In the study, the researcher relied mostly on the closed-ended questions because they provide greater uniformity of responses which can easily be subjected to statistical analysis.

3.4.4 The Interview Guide

An interview guide was also structured to elicit data that could not be obtained using the questionnaire. Leedy and Ormond (2005) cited in Salas (2009:71) contends that an interview is simply a questionnaire where the respondent is giving information orally. The interview is more intimate and has the advantage that the researcher pre-determines the topics and issues to be covered in advance. The researcher may also ask follow-up questions for clarification of salient points during the interview and can record the interview electronically. Salas (2009) also believes the interview allows for the understanding of live experiences and perceptions of the individuals experiencing the specific phenomenon. In this research, the interview guide was used to a less extend to interview some respondents.

3.4.5 Pre-Contacting of Respondents

Salkind (2010) contends that, to increase the response rate, a researcher must attempt to conduct the respondents prior to the administration of questionnaires and interviews through personal visits or telephone calls. A pre-contact involves the researcher identifying himself to the respondent, stating the purpose of the study and appealing for respondent's cooperation. Pre-contacts were effective in alerting the respondent to the imminent arrival of the questionnaire or a scheduled interview. This helped in gaining the respondent's cooperation and psyching them up on the issue under study.

3.4.6 Follow-up Activities

According to Salkind (2010:502), follow-up activities are necessary to improve the respondents' response rate. He suggests that if the response rate is to be less than 65%, the validity of the conclusions were considered to be weak. Consequently, the researcher took every effort to follow up and so improve the response rate to levels above the 65% threshold. In this regard, the researcher considered that a response rate that is below 65% would warrant follow-up activities with the respective target sample members in order to improve the response rate.

3.5 Data Collection, Analysis and Presentation

3.5.1 Data Collection

Data was collected by means of questionnaires that were hand delivered to the various respondents. Interviews were also conducted with directors (or the deputy in the absence of the director) of Finance, Procurement, IT, Military Police and Pay in order to obtain information relating to the areas of significant risks in their various departments.

3.5.2 Data Presentation, Analysis and Interpretation

Most of the data was presented in the form of tables, graphs and charts. After presentation, the data was analyzed using the mode and descriptive statistics. The researcher interpreted the data using inferential analysis and made recommendations accordingly.

3.6 Summary

In summary, the chapter outlined the research methodology, research design, determined the population and sample sizes, the sampling techniques and procedures utilised to analyse data. The chapter also looked at the instrument design that was used to assess data in terms of its validity and reliability. Data collection procedures and its presentation were also covered. Chapter 4 intends to cover data presentation, analysis and interpretation.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.0 Introduction

This chapter contains presentation, analysis and interpretation of data collected from various sources. It shows the statistical results of the questionnaires and interviews that were administered and conducted within the identified sample size. As already alluded to in Chapter 3, the researcher utilised tables, charts and graphs to depict data collected in order to facilitate data analysis and interpretation. The essence of this chapter is to answer the research questions as identified in Chapter one, and ends with a summary.

4.1 Research Findings

4.1.1 Response Rate From Questionnaires

The response rate in respect of questionnaires was 97.3% after having sent out 36 questionnaires and managed to get 35 questionnaires back. Given the high response rate, it can therefore be conclusively stated that the validity of the research outcomes is beyond doubt. The summary of responses are indicated on Table 4.1 below:

Table 4.1 Response Rate From Questionnaires

Department of Respondents	**Sample**	**Actual Responses**	**Non Response**	**Percentage of Responses**
Finance	5	5	-	100%
IT Directorate	5	5		100%
Military Police	5	5		100%
Pay	8	7		100%
Procurement	5	5	-	100%
Internal Audit	8	8		88.89%
Total	**36**	**35**		**97.3%**

According to Salkind (2010:502) and Babbie (2012:173), the threshold of a 'very good' response rate that is acceptable to represent the population from questionnaires must be at least 65% and 70% respectively. Thus, in the researcher's opinion, the response rate was highly remarkable and makes the research highly reliable and valid taking into account that questionnaires are normally associated with low response rate.

4.2 Tenets of a Risk Management Framework

The researcher sought to gather information that answers the research objective of the what constitute the tenets of a sound risk management framework. Respondents were required to indicate whether the ZNA has an integrated RM policy, an audit committee, identify stakeholders in RM, state the role of the commander and IA in RM. Table 4.2 below is a summary of the responses in respect of the five sub-research questions of the first objective.

Table 4.2 Tenets of a Risk Management Framework

Sub Research Question	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Total
There is an integrated RM policy in the Army	1 **2.86%**	6 **17.14%**	18 **51.43%**	10 **28.57%**	-	35 **100%**
There is an established RM committee in the Army	2 **5.72%**	8 **22.86%**	16 **45.71%**	9 **25.71%**	-	35 **100%**
RM is an all stakeholders' responsibility	19 **54.28%**	15 **42.86%**	1 **2.86%**	-	-	35 **100%**
IA advise commanders at all levels on RM processes	18 **51.42%**	15 **42.86%**	1 **2.86%**	1 **2.86%**	-	35 **100%**
There is a dedicated RM unit in the ZNA	5 **14.29%**	6 **17.14%**	11 **31.43%**	13 **37.14%**	-	35 **100%**

Table 4.2 shows that 28.57% of the respondents indicated that there is no integrated risk management policy in place in the ZNA. 51.43% of the respondents were indifferent while the remaining 20% (2.86% + 17.14%) believe that a risk management framework is available. The absence of an integrated RM framework was corroborated by 80% of the interviewees who echoed that there was need to have such a framework in the Army.

However, it was apparent that the various standing orders in place (especially those relating to security, guard, fire, IT, Pay, Finance, etc) are testimony of the semblance of a risk management framework, albeit a decentralized system. Such a disjoint in the risk management framework is contrary to the tenets of a sound ERM framework as proposed by various authorities (COSO, 2004 cited in Fraser and Henry, 2007; Griffiths, 2013; Little, 2013 cited in Schroeder, 2014:29; Castanheira, Rodrigues and Craig, 2010 and Miksen, 2014). These proponents indicated that there must be an integrated RM policy that coordinate all the players within the entity's structures. They assert that such a policy must spell out responsibilities of management, departments, internal audit and every member of the entity must be risk conscious.

4.3 Role of IA in Risk Management

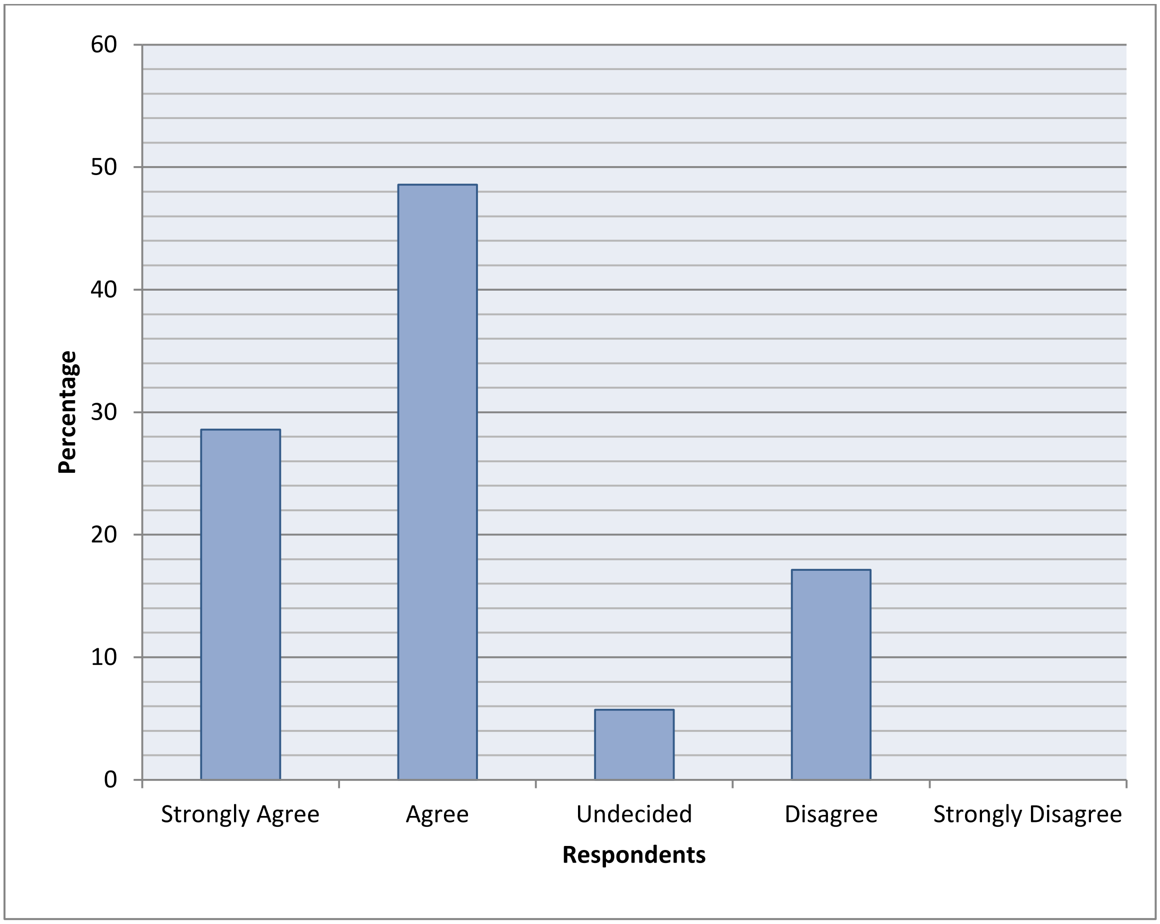
It was pertinent that the researcher seek respondents' views on the responsibilities of an IA function within the framework of RM. Three sub-research questions were therefore crafted for respondents to indicate what they believe should be the duties and responsibilities of the Army Internal Audit Department in RM. Table 4.3 below shows the respondents' views pertaining to the role of IA within the RM framework.

Table 4.3 Role of IA in Risk Management

Sub Research Question	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Total
IA regularly reviews risks to assets and resources	10	17	2	6	-	35
IA identify RM weaknesses in the ZNA's RM and recommend improvements	9	21	2	3	-	35
IA regularly runs RM workshops in the ZNA	-	-	11	20	4	35

Each of the three RM responsibilities of an IA function on Table 4.3 above are shown graphically in percentages on the following three graphs:

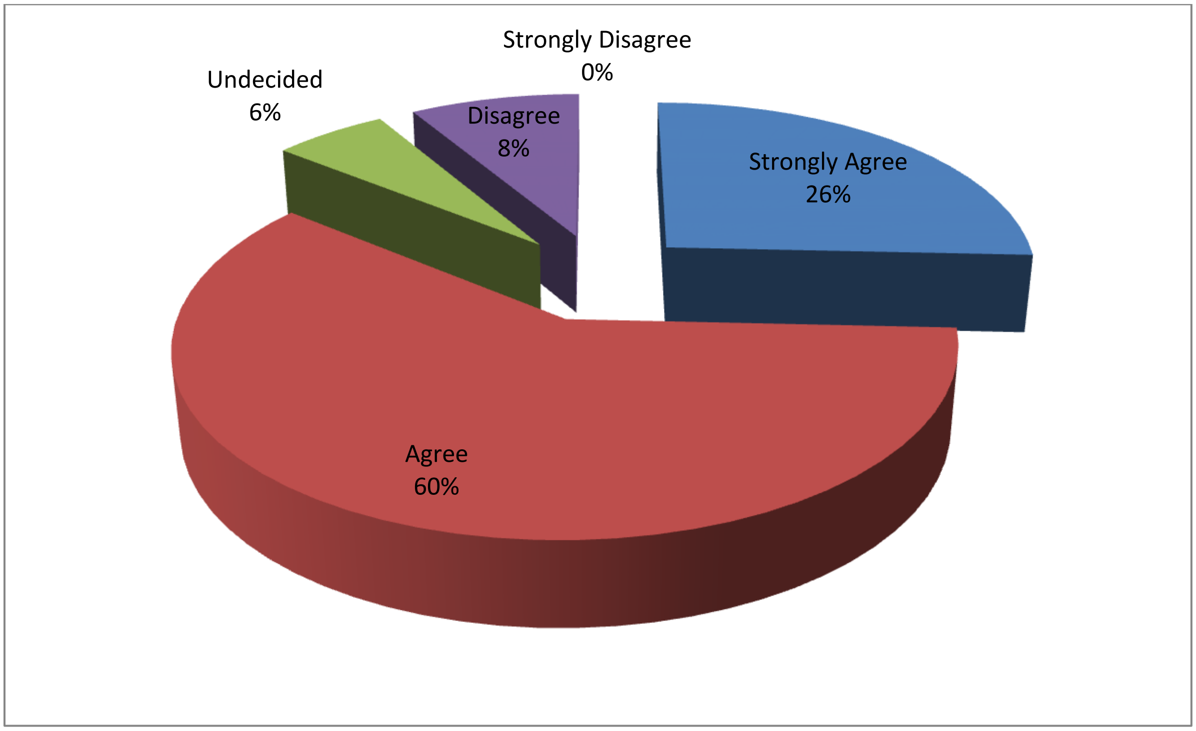
Figure 4.1 IA Reviews Risks to Assets and Resources



Source: Table 4.3

Figure 4.1 clearly shows that a total 77.14% (28.57 + 48.57%) of the respondents agree that the IA department is responsible for reviewing the risks that the ZNA's assets and resources are exposed to while 5.72% are undecided and 17.14% disagree. Available literature indicate that the IA function is responsible for carrying out such risk reviews to an entity's resources and assets in order to assist the organisation achieve its objectives (Griffiths, 2013; IIA (2004) cited in Fraser and Henry, 2007; and section 80 of the PFMA Chapter 22:19).

Figure 4.2 IA Identifies Weaknesses And Recommend Improvements

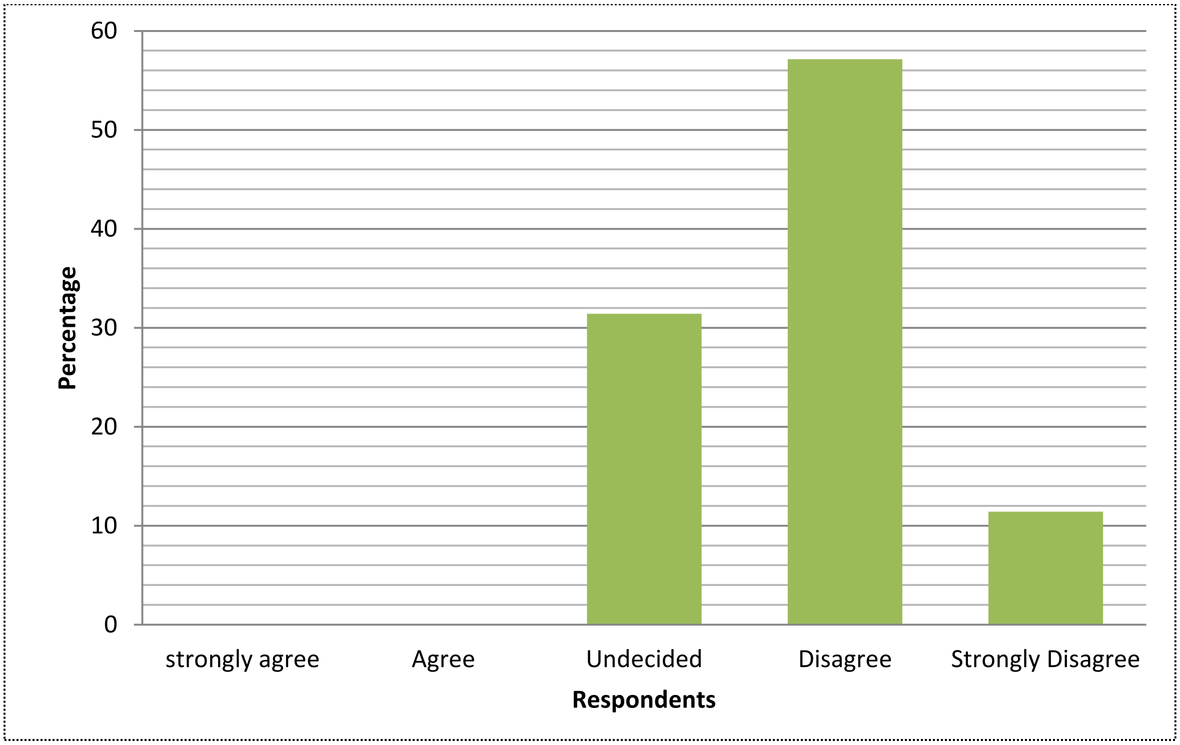


Source: Table 4.3

Figure 4.2 shows that a total of 86% (i.e. 26%+60%) of the respondents agree that the role of IA include identifying weaknesses and making recommendations for improvements. However, about 6% of the respondents are undecided while a further 8% disagrees that IA performs this function.

Clearly the majority of respondents are supported by available literature that IA identifies weaknesses and suggest recommendations to responsible officials. It is quite apparent that the IA gives an objective assurance that the entity's risks are being managed to acceptable levels. It gives this assurance by reviewing the effectiveness of the internal control system and recommending areas of improvement (Griffiths, 2013; IIA (2004) as cited in Fraser and Henry, 2007; King III Report, 2009; and section 80 of the PFMA).

Figure 4.3 IA Runs Risk Workshops in the ZNA



Source: Table 4.3

Figure 4.3 shows clearly that no respondent believes that Army Internal Audit Department has ever carried out any risk management workshops to coach ZNA members of the risk responsibilities. 31.43% are undecided as to whether the department carries out this function. 57.14% disagree and the remaining 11.43% strongly disagree that ZNA members have ever been coached of their risk responsibilities in any workshop.

From available literature review, it is clear that the running of risk workshops is done by a dedicated risk management unit, where such a unit exist. Alternatively, an audit committee can perform this function, or delegate this duty to the IA (Griffiths, 2013; IIA (2004) as cited in Fraser and Henry, 2007; King III Report, 2009). It is fairly apparent from an analysis of respondents' data that the IA is lacking in this area as it has never spearheaded any RM training program for ZNA members. This is somewhat understandable given the fact that there is no RM policy in place in the Army.

4.4 Adequacy of Risk Management Structures in the ZNA

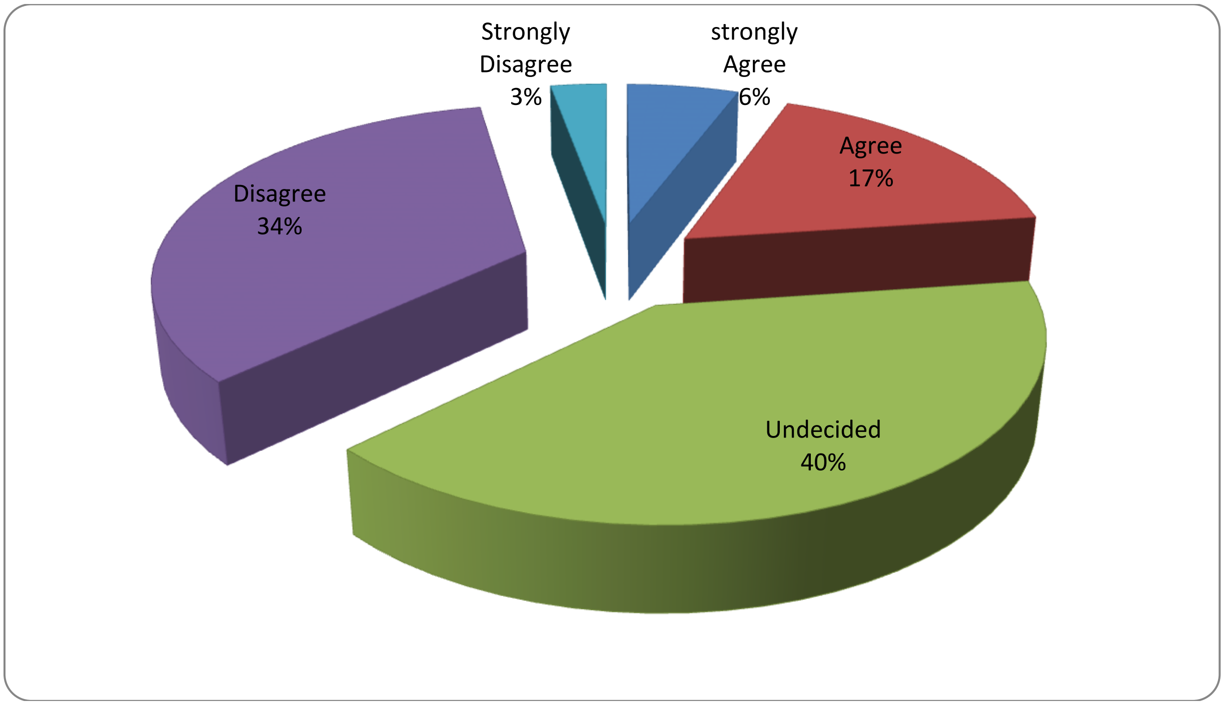
Notwithstanding the fact that there is no documented and approved RM policy, it was necessary to assess the adequacy of RM structures within the ZNA. To achieve this, the researcher sought respondents views on the adequacy or otherwise of the decentralized RM structures to address areas of heightened risks. Table 4.4 below is a summary of respondents' views pertaining the adequacy of RM structures in the Army:

Table 4.4 Adequacy of RM Structures to Address the ZNA's risk Profile

Sub Research Question	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Total
An elaborate RM structure exist which adequately address the ZNA's risk profile	2	6	14	12	1	35
A RM framework has been developed to address areas of heightened risk	2	8	14	11	-	35
It is necessary to adapt contemporary RM processes in the ZNA	9	25	1	-	-	35
It is necessary to appoint a RM official to champion the development of a RM policy	10	23	2	-	-	35

The researcher sought respondents views on the adequacy of RM structures in the Army. The responses are indicated on the pie charts below:

Figure 4.4 Adequacy of RM Structures in the ZNA

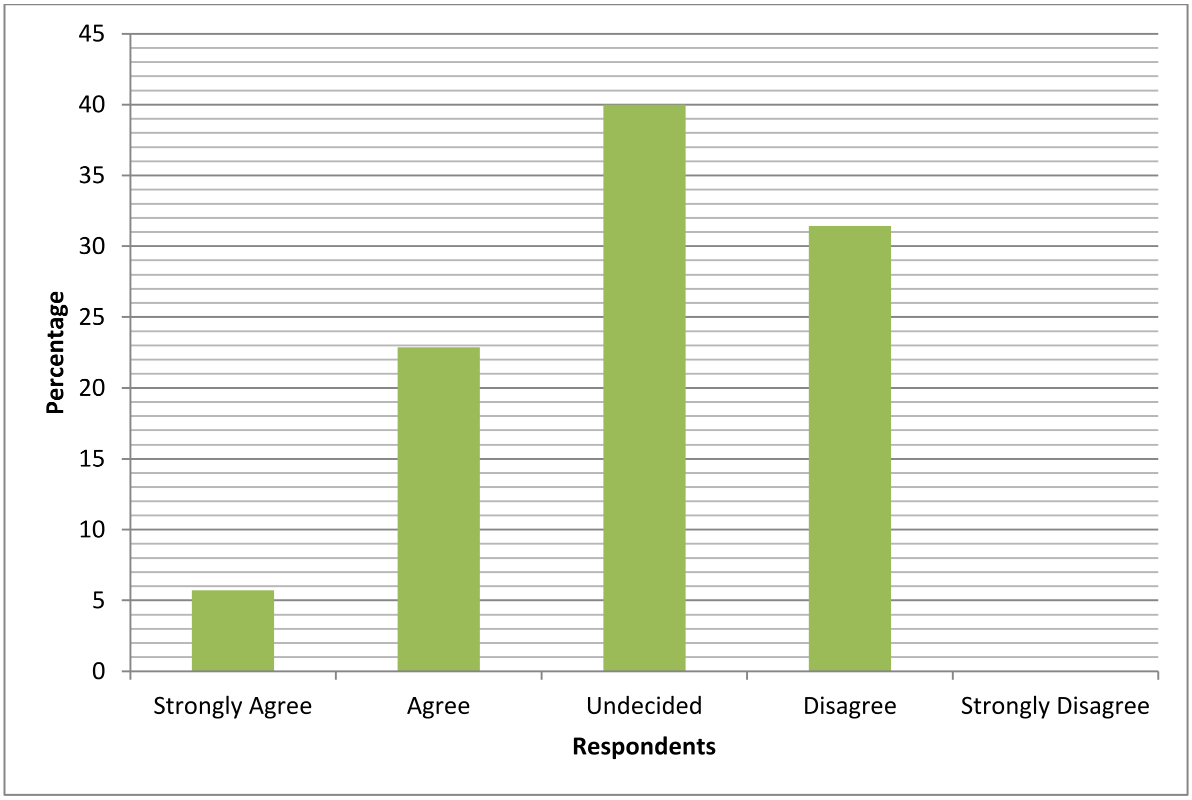


Source: Table 4.4

Figure 4.4 indicate that a total of 23% of the respondents agree, 40% are undecided and a total of 37% disagree that the RM structures in the ZNA are adequate. Clearly the undecided and those that disagree constitute the larger percentage of 77%. As such, it can be inferred that the RM structures in the ZNA are inadequate. This is true given the fact that there is no documented and approved RM policy that spell out the duties and responsibilities of key personnel and the various hierarchical structures in the Army.

According to Schroeder (2014:29) every employee must play a part in risk management. Schroeder also believes that a risk manager can be appointed whose duty would include ensuring that risk management is properly integrated into the business strategy. The IIA as cited in Fraser and Henry (2007) recognises different RM structures which include management, audit committee, department heads, internal audit. These structures perform specific responsibilities within the risk management framework of an entity. Unfortunately these structures are non-existent in the ZNA.

Figure 4.5 RM Framework was Developed to Address Areas of High Risk



Source: Table 4.4

Figure 4.5 indicates that a total of 29% (6%+23%) of the respondents agree that there is a RM framework of some sort which addresses areas of significant risk. 40% are undecided while 31% disagree that there is a RM framework in the Army. This was an area of doubt which needed interviews to clarify. Following interviews, it was established that a decentralized framework of risk management is in place to manage risk relating to areas of heightened risk at departmental levels.

From literature review, it was highlighted that areas of significant risk must be identified by management. In turn, management must then institute some processes (i.e. internal controls) to manage these areas. It was also highlighted that, since resources are seldom plentiful, the few resources available must be channeled towards managing the areas of heightened risk rather than spreading the meager resources thinly on small and trivial risks (Tummala and Schoenherr, 2011:476).

Whilst interviews managed to bring out that the existence of standing orders that outline the rules and regulations relating to the receipting, custody, sale, disposal and safeguarding of ZNA assets, it is incumbent that all these standing orders should have been extracts from the main RM policy framework. Consequently, it is concluded that an integrated RM policy document must be crafted in order to harmonise all these subsidiary RM frameworks.

4.5 Areas of Significant Risk

Questions were asked to source data from respondents on whether they believe IT, Pay, Finance, procurement, organisation culture and governance are indeed areas of significant risk to the ZNA as highlighted during literature review (Rubino and Vitalla, 2013; Pramod, Li and Gao, 2012; Schroeder, 2014; and King 3 Report, 2009).

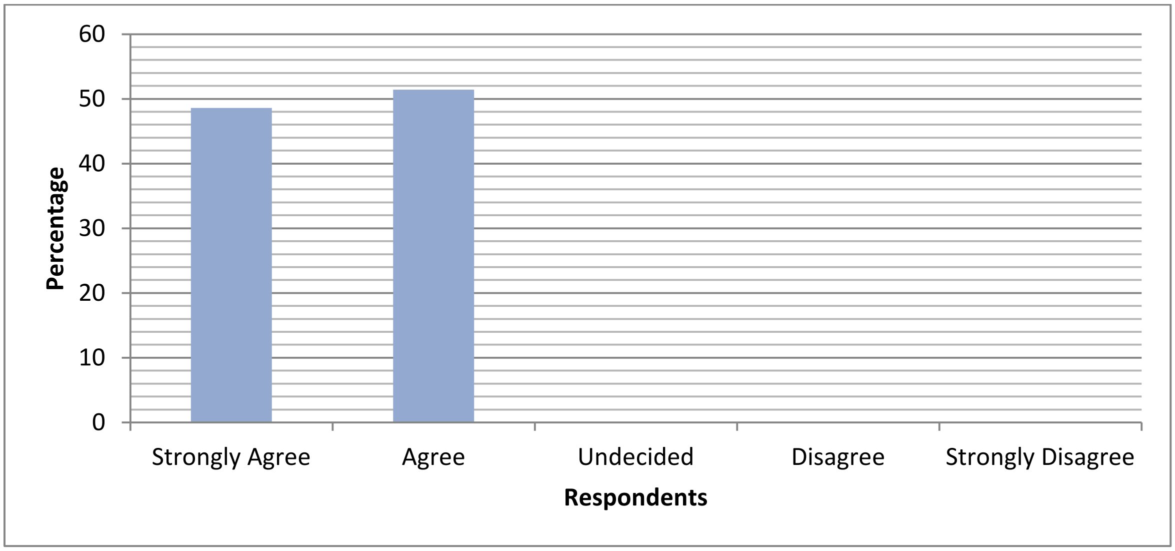
The respondents' views are capture on Table 4.5 below:

Table 4.5 Areas of Significant Risk to the ZNA

Sub Research Question	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Total
IT and Pay departments are some of the areas of significant risk	17	18	-	-	-	35
Finance and Procurement departments are some of the areas of significant risk	17	17	1	-	-	35
Organisation culture and governance are some of the areas of significant risk	4	25	4	2	-	35

Figure 4.6 below graphically illustrate respondents' views regarding IT and Pay as areas of significant risk as previously identified in literature review in Chapter two:

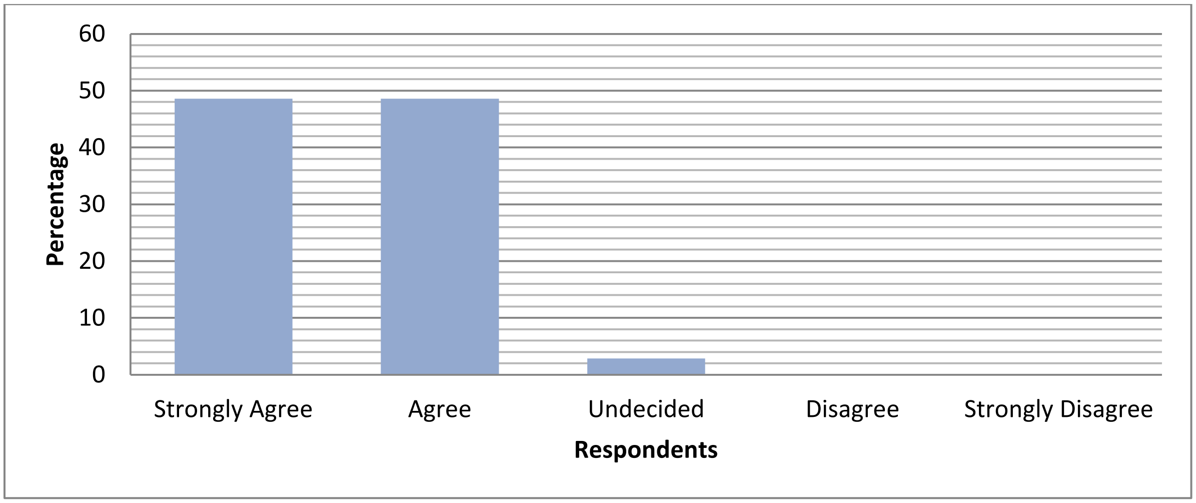
Figure 4.6 Respondents Views on IT and Pay Directorates



Source: Table 4.5

Figure 4.6 clearly indicate that 100% of the respondents agree that IT and Pay directorates are areas of significant risk. This trend corroborates what has been suggested during literature review by other authorities (Rubino and Vitalla, 2013; Pramod, Li and Gao, 2012; Schroeder, 2014; and King 3 Report, 2009).

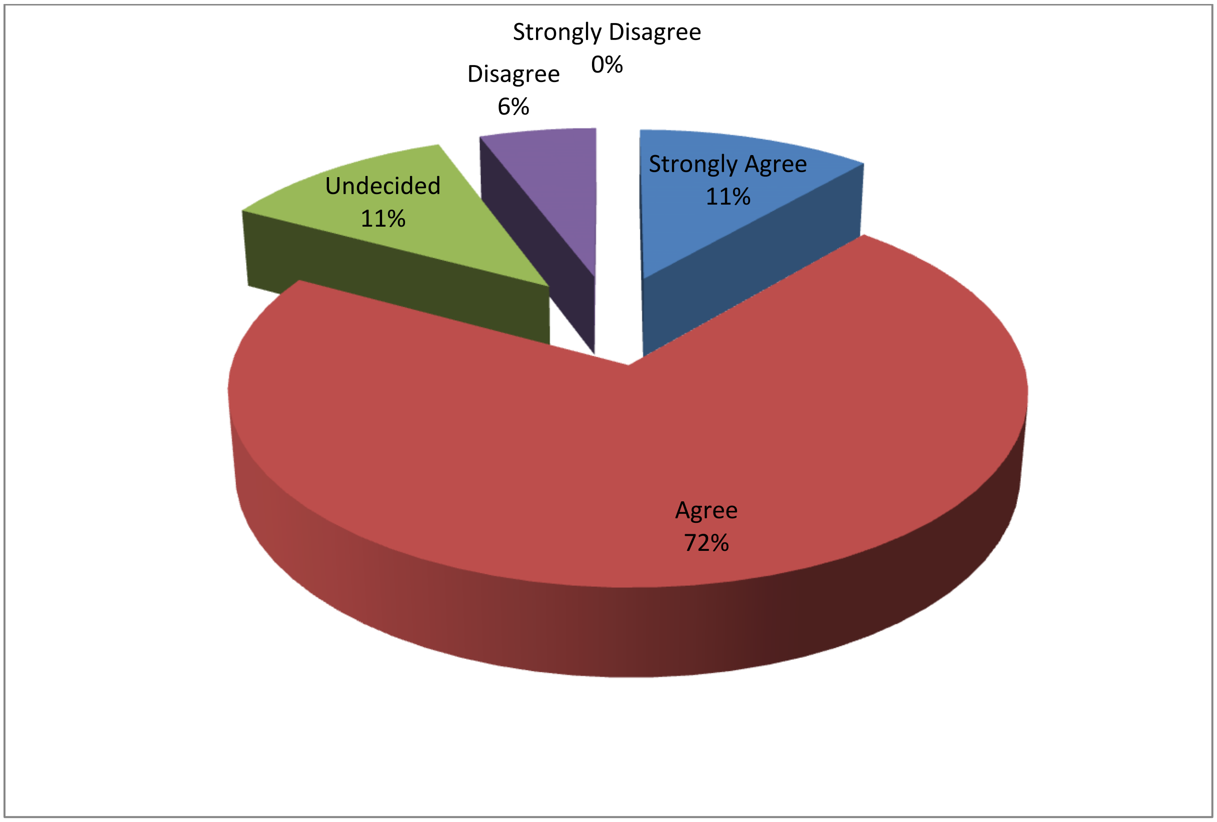
Figure 4.7 Respondents Views on Finance and Procurement Directorates



Source: Table 4.5

Figures 4.7 clearly indicate that 97% of the respondents agree that Finance and Procurement departments are areas of significant risk. This trend exhibited by the majority of the respondents conforms to what was claimed by other authorities during literature review (Rubino and Vitalla, 2013; Pramod, Li and Gao, 2012; Schroeder, 2014; King 3 Report, 2009; and the Minister of Finance Mr. P Chinamasa, 2013).

Figure 4.8 Respondents Views on Culture and Governance



Source: Table 4.5

Figures 4.8 clearly demonstrate that 83% (i.e. 72% + 11%) of the respondents agree that organisation culture and governance are areas of significant risk to the ZNA. This tendency tallies with what has been suggested during literature review by other authorities (Schroeder, 2014; King 3 Report, 2009; and the Minister of Finance Mr. P Chinamasa, 2013).

4.6 Suggested Risk Management Model

The researcher sought views of respondents on how the ZNA should formulate its risk management model. Cognizant of the fact that the ZNA is an arm of national security, it may not be feasible to reproduce risk management models that have been proposed for private entities. The fact that ZNA is exposed to risk, it therefore follows that a risk management model of some kind is indispensible. Consequently, the researcher inquired from respondents whether or not the ZNA should adapt the risk models that have been proffered by some authorities. Table 4.6 below tabulates the views of the respondents:

Table 4.6 Suggested Risk Management Models

Sub Research Question	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree	Total
It is necessary to identify areas of significant risk and manage them	22	13	-	-	-	35
IA should concentrate on areas of significant risks because resources are not enough	12	13	4	1	-	35
Establishing a RM unit is necessary in the ZNA	13	17	4	1	-	
When resources are not enough they should be used to manage areas of significant risk	18	14	1	1	1	35

From Table 4.6 above, it is clear that all the respondents agree that areas of significant risk must be identified and managed. This is because an organisation cannot always have enough resources to spread all over to cover trivial and small risks.

80% of the respondents interviewed contend that the ZNA should not re-invent the wheel but adapt any one of the many risk management models in order to suit its own peculiar circumstances. It was suggested that a board be constituted by command element which should be guided by clearly spelt out terms of reference. Such a board must recommend any of the RM best practices as articulated by Griffiths (2013); IIA (2004); COSO framework, CIIA of Australia (2012); Turnbull Review Group (FRC, 2005); Castanheira, Rodrigues and Craig (2010); and Tummala and Schoenherr (2007).

It was also suggested that, since the entire Ministry of Defence does not have a RM policy, it would be prudent to engage a consultant to assist in the formulation and integration of RM into the ministry's strategy.

4.7 Response Rate on Interviews

Interviews were conducted to fill in gaps of information and knowledge that became apparent after the analysis and interpretation of data obtained from questionnaires. The response rate on interviews provide reassurances that the information obtained from questionnaires can be projected to the entire population from which the sample was drawn. Babbie (2012) suggests that a 75% response rate on interviews is acceptable to be representative of the population. Tabulated below on Table 4.7 is the response rate on interviews:

Table 4.7 Response Rate From Interviews

Director/Deputy Director	Scheduled Interview	Interview Done	% Response Rate
Finance	1	1	100%
IT	1	1	100%
Procurement	1	1	100%
Pay	1	1	100%
Internal Audit	1	-	0%
Military Police	1	1	100%
Total	**6**	**5**	83.3%

Table 4.7 shows that the response rate from interviews was 83.3%. The researcher targeted directors or deputy directors of the departments of the purposive sample selected for questionnaires in order to clarify certain gray areas that became apparent during the questionnaires.

4.7.1 Interview Responses

80% of the interviewees indicated that there is need to formulate an integrated RM policy from which all the departments will draw their risk responsibilities. 20% believed that the current arrangement where there are standing orders is adequate to manage risk. Of the 80% who advocate for the formulation of RM policy, 50% suggested adapting any one of the RM models available while the other 50% suggested engaging a consultant. 40% of the respondents indicated that it was necessary to establish a dedicated RM unit in the Army while the remaining 60% contend that the RM structures must just be embedded within the ZNA structures. Embedding RM within an entity's structures conforms with proposals by other authorities (Griffiths, 2013 and the IIA as cited by Fraser and Henry, 2007).

All the interviewed respondents agree that IT, Pay, Finance and Procurement are areas of significant risk. This trend corroborates the various authorities which cited these departments as high risk areas (Rubino and Vitalla, 2013; Pramod, Li and Gao, 2012; Schroeder, 2014; King 3 Report, 2009; and Chinamasa, 2013).

4.8 Review of Secondary Data

The absence of an integrated RM policy in the ZNA was corroborated by secondary data from the Office of the Auditor General in their audit of the ZNA's 2013 Appropriation Account. The Auditor General observed that the ZNA has no documented and approved risk management policy to effectively identify, assess, manage and mitigate risks to its operations as required by good corporate governance principles (Office of the Auditor General Audit Query Number 5 dated 03 July 2014).

4.9 Summary

The results show that ERM structures are disintegrated and in some cases non-existent. As recommended by most respondents, the ZNA should consider putting in place an integrated risk management framework which clearly articulate the risk responsibilities of command element, audit committee, internal audit, commanders at all levels and every member of the force. It is desirable that an audit committee is appointed to champion the formulation of an integrated risk management policy and also spearhead the coaching of members across the rank and file so that they are all risk conscious.

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

The purpose of this chapter is to summarise the findings, come up with conclusions of the study and finally recommend the internal audit model that can be used by the Army Internal Audit Department in carrying its internal audit function.

5.1 Summary of Chapters

5.1.1 Chapter One

This chapter highlighted the ever-increasing need for corporations, both private and public, to manage risk. The IA's continued use of the traditional compliance based audit approach has not managed to reduce risks to acceptable levels. Control based internal auditing approach has so far failed to prevent, detect and correct internal control weaknesses as evidenced by the increase in criminal cases in the Army. As such, the researcher sought to suggest a paradigm shift by investigating the challenges of implementing the contemporary RBIA in the ZNA with a view to reducing the ZNA's risk exposures.

5.1.2 Chapter Two

Chapter Two reviews literature from books, magazines and journal in order to answer the research questions identified in chapter one. The reviewed literature indicates that RBIA is premised on the concept of risk management. Hence, the role of the IA's function of providing an objective assurance that risks are being managed to acceptable levels is largely dependant on the nature, scope and magnitude of risks that an entity is exposed to. Consequently, for the IA to carry out this function efficiently, effectively and economically, it has to adopt the more contemporary RBIA approach.

5.1.3 Chapter Three

Chapter Three looked at the research methodologies that were used to gather data in order to answer the research questions. The researcher utilised the case study, descriptive and survey research instrument designs to gather data. Closed-ended questionnaires and interviews were administered and conducted on the target sample purposively selected. The response rate in respect of both the questionnaire and interviews were quite remarkable (above 80%), and consequently the researcher is convinced the research outcomes are valid and reliable.

5.1.4 Chapter Four

Chapter Four was concerned with data presentation, analysis and interpretation. The researcher utilised tables, charts and graphs to depict data collected in order to facilitate analysis and interpretation. It was also possible to review secondary data to corroborate the findings from questionnaires and interviews.

5.1.5 Chapter Five

Chapter Five intends to summarise the chapters and major findings, conclude and make recommendations.

5.2 Major Findings

The research found out that:

5.2.1 Tenets of a Risk Management Framework

The ZNA has no documented and approved RM policy. It is important that an integrated RM policy is put in place that spell out the responsibilities of command element, departments, internal audit, and every member of the force. However, there are fragmented standing orders that regulate the operations of individual departments. An integrated RM policy will ensure that each department extracts its risk responsibilities from the main authoritative document if it is put in place.

5.2.2 The Role of IA Within the Risk Management Framework

It was established that the role of the IA is to identify, assess and review risks. The IA is also responsible for identifying weaknesses and making recommendations for improvements to management. However, the IA has not run any risk workshops before to coach member of risk best practices and to ensure that every member is conscious of their risk responsibilities.

5.2.3 Risk Management Structures

The ZNA has no established RM structure with clearly defined responsibilities for command element, audit committee, internal audit, department heads and every member in the force. Departments administer decentralized standing orders within their respective spheres of work environments for which management has not defined its desired risk appetite. Command element should define its risk appetite to the respective departments and demand that each department manages risk within the defined appetite level.

There is no dedicated risk management unit to spearhead risk management in the Army. The ZNA has high value and high risk assets and resources in its inventory which require to be managed judiciously and prudently. By establishing a dedicate risk management unit or committee, the ZNA is able to ensure that risk management is embedded within the existing ZNA management structures.

5.2.4 The Adequacy of RM to Address the ZNA's Risk Profile

The ZNA's risk management architecture is inadequate to address the ZNA's risk exposures. There is no integrated risk management policy, no dedicated risk structures, no deliberate risk management training and there is no defined risk appetite. A risk management policy has to be put in place, risk structures have to be established, risk management training has to be done to make every member conscious of their risk responsibilities and management should define its risk appetite to subordinate departments.

5.2.5 Areas of Significant Risk

The research found out that the directorates of IT, Pay, Finance and Procurement, as well as organisation culture and governance, are areas of significant risk to the Army. Without clearly defined areas of heightened risk, management and IA's efforts to minimise risk would be thinly spread across the whole departments of the organisation. Doing so would imply that there is no cost-effect utilization of the organisation's finite resources. As a result, resources must be used where they derive the most impact because they are rarely plentiful.

5.2.5 Suggested Risk Management Models

There is no risk management model in place in the ZNA and the entire Ministry of Defence at large. It is suggested that the ZNA, and indeed the entire Ministry of Defence, should formulate an integrated risk management policy which feeds into their overall strategy. The ZNA can engage a consultant to help it formulate a RM policy. Alternatively, it can constitute a board to look at risk models propounded by different authorities and adapt any one or a hybrid that meets its peculiar circumstances.

5.3 Conclusion

The researcher is quite convinced that the research was a resounding success. This is because the response rate from questionnaires was 97.2% while that of interviews was 83.3%. Such a response rate exceeds the acceptable threshold of 65% and 70% as stated by Salkind (2010:502) and Babbie (2012:173) respectively. As such, reliable and valid assertions can be drawn from the sample population given the very good response rate. In addition, the purposive sample of officers selected for questionnaires and interviews have managed to bring in insightful observations and recommendations.

Also, it is the researcher's conviction that all the objectives that the research set out to be achieved in first chapter, were achieved. There abundant literature reviewed contributed by bringing in many insightful theories, concepts and views that overall helped in exposing the objectives of the study. Consequently, it was possible to relate available literature with the responses from the many respondents and draw reliable and valid conclusions.

5.4 Recommendations

The researcher recommends that:

5.4.1 The ZNA should formulate an integrated risk management policy document. This is because the ZNA does not have a documented and approved risk management policy to effectively identify, assess, manage and mitigate risks to its operations as required by good corporate governance principles.

During the review of literature, 28.6% of the respondents indicated that there is no integrated risk management policy in place in the ZNA. 51.4% of the respondents were indifferent while the remaining 20% believed a RM framework was available. However, it was apparent that the various standing orders in place (especially those relating to security, guard, fire, IT, Pay, Finance, etc) are testimony of the semblance of a risk management framework, albeit a decentralized system. Such a disjoint in the risk management framework is contrary to the tenets of a sound ERM framework as proposed by various authorities (Griffiths, 2013; COSO, 2004 cited in Fraser and Henry, 2007:393; and Little, 2013 cited in Schroeder, 2014:29).

Also, the Office of the Auditor General, in their audit of the ZNA's 2013 Appropriation Account, observed that the ZNA has no documented and approved risk management policy to effectively identify, assess, manage and mitigate risks to its operations as required by good corporate governance principles (Office of the Auditor General audit query number 5 dated 03 July 2014).

5.4.2 The IA should run risk workshops to train all members within the rank and file so that they are conscious of their risk responsibilities. Available literature indicate that, in the absence of a dedicated RM unit or committee, the IA function should perform this function (Griffiths, 2013; COSO, 2004 cited in Fraser and Henry, 2007:393; and Little, 2013 cited in Schroeder, 2014:29). However, the respondents overwhelmingly (i.e. 100%) indicated that the IA has never run such kind of training. The responses by the majority of the respondents actually attests to the fact that most members of the force are risk naïve. This contradicts the IA role of coaching staff in risk management 'best practices' as articulated by Griffiths (2013:5).

The IA should embark on a deliberate training program to acquire risk management skills and attitudes in order to be able to discharge of this mandate. This may also entail establishing an audit team specifically trained in risk management which would audit the risk management structures and processes in the Army.

Also, Griffiths (2013) and the PFMA section 84, identify the responsibility of an audit committee as that of reviewing internal controls, including the scope of internal audit program, its findings, and to recommend appropriate action to be taken by responsible officials. This implies that the audit committee utilises the IA department to review management's processes to manage risk to acceptable levels.

5.4.3 The ZNA should establish risk management structures with clearly defined responsibilities for command element, audit committee, internal audit, department heads and every member in the force. Authorities Rubino and Vitalla (2013); Pramod, Li and Gao (2012); Schroeder (2014); and King 3 Report (2009) believe that these structures are necessary for any risk management framework. This also confirmed by Schroeder (2014:29) who assert that risk management is an all stakeholders' responsibility where every employee must play a part.

5.4.4 The ZNA should designate the departments of IT, Pay, Finance and procurement as areas of significant risk together with organisation culture and governance. This is confirmed in literature review where it was clearly indicated that IT, Pay, Finance, Procurement, organisation culture and governance are indeed areas of significant risk (Rubino and Vitalla, 2013; Pramod, Li and Gao, 2012; Schroeder, 2014; King 3 Report, 2009; and the Minister of Finance Mr. P Chinamasa, 2013).

5.4.5 The Ministry of Defence in general and the ZNA in particular should formulate an integrated risk management policy which feeds into its overall strategy. The policy can be formulated by adopting one of two options:

- Option one

To engage a consultant to assist in the formulation of a risk management policy that is dovetailed to meet the peculiar circumstances of the ministry.

- Option two

To constitute a board which looks at all the available risk management models and adapt one, or a hybrid, that meets its peculiar circumstances.

If option two is adopted, it is suggested that command element clearly spell out the terms of reference for the board so that it recommends some of the RM best practices as articulated by RM gurus such as Griffiths (2013); IIA (2004); COSO framework, CIIA of Australia (2012); Turnbull Review Group (FRC, 2005); Castanheira, Rodrigues and Craig (2010); and Tummala and Schoenherr (2007).

BIBLIOGRAPHY

Books

Babbie, ER. (2006), *The Practice of Social Research*. Belmont: Wards Worth Publishing.

Cohen, L., Manion, L., Morrison, K. and Morrison, R.B. (2007), *Research Methods in Education.* London: Routledge.

Frankel, J. and Wallen, NE. (2006), *How to design and evaluate research in education.* New York: Von Hoffman.

Hardy, K. (2010), M*anaging risk in government: An introduction to enterprise risk management.* 2nd Ed Financial Management Series: IBM Center for the Business of Government.

Jackson, SL. (2009), *Research methods and statistics: A critical thinking approach.* 3rd Ed, Belmont, CA: Wadsworth.

Salkind, NJ. (2010), *Encyclopedia of Research Design.* Vol. 1 Sage Publications: Amazon.com.

Saunders, M., Lewis, P. and Thornhill, A. (2007), *Research methods for business students.* 4th Ed. London: Prentice Hall Publications.

The Audit Office Act Chapter 22:18 of 2009

The Public Finance Management Act Chapter 22:19 of 2009.

VanderStroep, SW. and Johnson, DD. (2010), *Research methods for everyday life: Blending qualitative and quantitative approaches."* London: John Wiley & Sons.

Walliman, NS. and Walliman, N. (2011), *Research Methods: the basics.* London: Taylor and Francis.

Wilsons, J. (2010), *Essentials of business research: A guide to doing your project.*" London: Sage Publications.

Yamagata-Lynch, LC. (2010), *"Activity systems analysis methods: Understanding complex learning environments."* New York: Springer Publications.

Journals

Castanheira, N. Rodrigues, L. and Craig, R. (2010). *Managerial Auditing Journal*. Vol. 25 No. 1 pp 79-98.

Chartered Institute of Internal Auditors (2014).

Chinweike, (2012). *What is Risk Based Auditing? Meaning, Process and importance of Risk Based Auditing*.

Colbert, J.L. and Alderman, C.W. (1995), "A Risk-driven approach to internal audit". *Managerial Auditing Journal* Vol.10 no. 2 pp 38-44.

Enofe, A.O., Mgbame, CJ., Osa-Erhabor, VE. and Ehiorobo, AJ. (2013), "The Role of Internal Audit in effective management in public sector." *Research Journal of Finance and Accounting*. Vol. 4 No. 6 pp 162-166.

Fraser, I. and Henry, W. (2007), "Embedding Risk Management: Structures and approaches". *Managerial Auditing Journal*. Vol. 22 No. 4 pp 392-409.

Institute of Chartered Accountants in Australia (2013).

Powers, M. (2010), "Where ignorance is bliss: the "dark corner" of risk classification". *The Journal Of Risk Finance,* Vol. 11 No. 4 pp 353-357.

Pramod, V., Li, J. and Gao, P. (2012), "A Framework for preventing money laundering in banks". *Information management and computer security,* Vol. 20. No. 3 pp 170-183.

Robinson, OC. (2010), "Sampling in interview-based qualitative research: A theoretical and practical guide", *Qualitative Research In Psychology*, pp 25-41.

Rubino, M. and Vitalla, F. (2014), "Corporate governance and the information system: how a framework for IT governance supports ERM", *Corporate Governance Journal* Vol. 14 No. 3 pp 320-338.

Salas, C. (2009), "The Influence of organisational structure on customer issue resolution. A phenomenological study", *ProQuest*.

Schroeder, H. (2014), "An art and science approach to strategic risk management", *Strategic Direction* Vol. 30. No.4 pp 28-30.

Tchankova, L. (2002), "Risk Identification- basic stage in risk management", *Environmental Management and Health Journal,* Vol. 13 No. 3 pp 290-297.

The King 3 Report, (2009), "The King Report on Corporate Governance for Southern Africa", *Institute of Directors in Southern Africa*: pp 31-49.

Tummala, R. and Schoenherr, T. (2011), "Assessing and managing risk using the Supply Chain Management Process", *Supply Chain Management: An International Journal*, 16/6 pp 474-483.

Ziegenefuss, DE. (1995), "The state of art in internal auditing risk assessment techniques", *Managerial Auditing Journal* Vol. 10. No. 4 pp 3-11.

Websites

Griffiths, D. (2013), "An introduction to Risk Based Internal Auditing", [Available: www.internalaudit.biz: Accessed 21 July 2014 at 15:23 hours].

The Business Dictionary, (2012). Available: [http://www.businessdictionary.com/definition/risk-management.html]: (Accessed 21 August 2014 at 15:45 hours).

Vaccaro (2014). Available: http://science.blurtit.com/23704/what-is-research-methodology-: [Accessed on 8 September 2014 at 15:22 hours].

Documents

The Office of the Auditor General's Report, (2014), Audit Query Number 5 on the audit of ZNA 2013 Appropriation Account.

APPENDIX 1

Copy No: of copies

Directorate of Army Finance
P Bag 7720
Causeway

Harare 793252

The Commander
Army Headquarters
P Bag 7720
Causeway

September 2014

Sir

REQUEST FOR AUTHORITY TO CARRY OUT RESEARCH WITHIN THE ZNA

1. Sir, I have the honour to apply for authority to carry out a research within the ZNA. The research project is a requirement in partial fulfilment of my studies for a Bachelor of Commerce Accounting Honours Degree programme with Midlands State University (MSU).

2. It is common university practice that any student undergoing a program of study must conduct a research in any one of the core modules prior to graduating. In this regard, the College has authorized one of my three dissertation proposals titled "An investigation of the challenges of implementing the Risk Based Internal Auditing (RBIA) approach in the ZNA." Should my request be authorized, I intend to sent out questionnaires and conduct interviews of various stakeholders within the ZNA, in particular, a sample of officers from the departments of Finance, Procurement, IT, Internal Audit, and Pay.

3. Sir, may it please you that the research and the resultant findings are required purely for academic purposes.

I have the honour to be,
Sir,
Your obedient Subordinate

V MACHAYA OZM 'psc' ZW
Lieutenant Colonel
Deputy Director Financial Accounting

[Student Registration No. R11289N]

APPENDIX 2

Directorate of Army Finance
P Bag 7720
Causeway

Harare 793252

Dear Respondent

September 2014

REQUEST TO COMPLETE A QUESTIONNAIRE

1. I, Lieutenant Colonel V Machaya, a Bachelor of Commerce Honours Accounting Degree student (Registration No. R11289N) at Midlands State University (MSU), am carrying out a research project in partial fulfilment of my degree program at MSU.

2. It is common university practice that any student undergoing a program of study must conduct a research in any one of the core modules prior to graduating. In this regard, the College has authorized my dissertation proposal on the topic *"An investigation of the challenges of implementing the Risk Based Internal Auditing (RBIA) approach in the ZNA"*.

3. Against this background, I am sincerely requesting you to participate in the research by completing the attached questionnaire. Your honest and sincere responses to this questionnaire would therefore be greatly appreciated.

4. I would like to assure you that this research and the resultant findings are required purely for academic purposes. As you take part in this survey, be rest assured that the information you will provide will be treated with strict confidence.

5. I thank you very much for your cooperation.

V MACHAYA OZM 'psc' ZW
Lieutenant Colonel
Deputy Director Financial Accounting

APPENDIX 3

QUESTIONNAIRE

Please respond by ticking on the blank space provided.

DEMOGRAPHY

a. Please indicate your gender.

Male □ **Female** □

b. Indicate your marital status

Married □ **Single** □ **Other** □

c. Identify your age group

20-30yrs □ **31-40yrs** □ **41-50yrs** □ **51yrs & over** □

d. Indicate your period of service in the ZNA

1-10yrs □ **11-20yrs** □ **21-30yrs** □ **30yrs & over** □

e. State your designation (rank)

Non-Commissioned Officer □ **Junior Officer** □ **Senior Officer** □

RESEARCH QUESTIONS

1. There is an integrated risk management policy in the Army.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

2. There is an established risk management committee in the ZNA to advice the command element (management) on risk management.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

3. Risk management is an all stakeholders' responsibility (i.e. the ZNA risk management structure has a role for the command element, the internal audit, and every department must have clearly defined responsibilities for risk management and every member in the ZNA must be risk conscious).

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

4. The Internal Audit department has a central role in advising commanders at all levels on risk management processes in the ZNA.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

5. There is a dedicated risk management unit in the ZNA.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

6. Command element gives Army Internal Audit Department direction to identify and assess the risks to assets and resources (including financial resources) on charge to the ZNA.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

7. The risks to assets and resources of the ZNA are regularly reviewed by Army Internal Audit Department.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

8. Army Internal Audit Department identify the weaknesses of the ZNA's risk management architecture and make recommendations for improvements.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

9. The Army Internal Audit Department regularly runs risk workshops to coach ZNA members of their risk responsibilities.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

10. The ZNA has an elaborate risk management policy which adequately address the ZNA's risk profile.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

11. A risk management framework has been developed to address areas of heightened risk.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

12. It is necessary to adapt contemporary risk management processes to suit the ZNA.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

13. It is necessary to appoint a risk management official to spearhead the development of an elaborate risk management framework for the Army.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

14. The IT and Army Pay Directorates are some of the areas of significant risk to the ZNA.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

15. The Finance & Procurement Departments are some of the areas of significant risk to the ZNA.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

16. Organisation culture and governance are some of the areas of significant risk to the ZNA.

Strongly Agree	**Agree**	**Undecided**	**Disagree**	**Strongly Disagree**
□	□	□	□	□

17. It is necessary to identify all areas of significant risk in the Army and manage them.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

18. Internal Audit Directorate should concentrate their audit on areas of significant risk because resources are seldom (rarely) plentiful.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

19. Establishing a risk management unit is necessary in the ZNA.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

20. When resources are inadequate, it is necessary to commit the few resources to managing significant risks than to commit the finite resources on small and trivial risks.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
□	□	□	□	□

Any other information you may have, put down here:

……
……
……

May you please stamp the first page using a unit date stamp. Thank You!!!

APPENDIX 4

INTERVIEW GUIDE

Department:……………………………………………….

RESEARCH QUESTIONS

1. The Auditor General noted that the ZNA does not have an integrated risk management policy framework. Do you think it is desirable (necessary) to establish such a policy? If yes, what kind of risk structure do you think the ZNA should establish and how should it be operationalized?

2. Can you identify the departments and the various roles that they should play in risk management in the Army?

3. Which unit should spearhead running of risk workshops to coach ZNA members of their risk responsibilities.

4. Why should the ZNA establish (or not establish) a dedicated risk management unit? If established, what would be the responsibilities and reporting protocol of such a unit?

5. Which areas or departments do you consider to areas of significant risk to the ZNA and why?

6. There are many models of risk management processes developed by a number of authors. Most of them a tailored for private entities. How should the ZNA develop its risk management framework?

7. Does the ZNA's culture and governance structures support well-thought through risk taking and innovation?

8. Are the risks associated with working with other organisations assessed and managed?

9. In his 2014 National Budget Statement, the Minister of Finance Mr. P Chinamasa (2013:115-118) underscored the need to strengthen governance and accountability in public resource management. The Minister noted the glaring shortcomings in the public procurement systems and suggested revamping the arrangements and processes to achieve efficiency, transparency, accountability and professionalism.

Do you think there is merit in the Minister's assertions?

10. Do you have any other information you may wish to say in connection with this matter?

………

………

………

………

May you please stamp the first page using a unit date stamp.

Thank You!!!